

By Senator Harrell

31-01058B-26

2026480

31-01058B-26

2026480

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

31-01058B-26

2026480

related projects; conforming a cross-reference; amending s. 282.0041, F.S.; deleting and revising definitions; defining the terms "DIGIT" and "technical debt"; amending s. 282.00515, F.S.; authorizing the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services to adopt alternative standards that must be based on best practices and certain standards; requiring the departments to evaluate the adoption of such standards on a case-by-case basis; requiring the departments to follow specified standards under certain circumstances; requiring the departments to conduct a certain full baseline needs assessment; authorizing the departments to contract with DIGIT to assist or complete such assessment; requiring the departments to each produce certain phased roadmaps that must be submitted annually with specified budget requests; authorizing the departments to contract with DIGIT to assist or complete such roadmaps; authorizing the departments to contract with DIGIT for specified services; requiring the departments to use certain information technology reports and follow a specified reporting process; requiring the departments to submit a certain report annually by a specified date to the Governor and the Legislature; revising applicability; authorizing DIGIT to perform project oversight on information technology projects of the departments which have a specified project cost; requiring that such projects comply with

31-01058B-26

2026480

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

31-01058B-26

2026480

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

31-01058B-26

2026480

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

31-01058B-26

2026480

175 requiring DIGIT, in consultation with state agencies,
176 to create a methodology, approach, and applicable
177 templates and formats for identifying and collecting
178 information technology expenditure data at the state
179 agency level; requiring DIGIT to continuously obtain,
180 review, and maintain records of the appropriations,
181 expenditures, and revenues for information technology
182 for each state agency; requiring DIGIT to prescribe
183 the format for state agencies to provide financial
184 information to DIGIT for inclusion in a certain annual
185 report; requiring state agencies to submit such
186 information by a specified date annually; requiring
187 DIGIT to work with state agencies to provide
188 alternative standards, policies, or requirements under
189 specified circumstances; creating s. 282.0062, F.S.;
190 establishing workgroups within DIGIT to facilitate
191 coordination with state agencies; providing for the
192 membership and duties of such workgroups; requiring
193 the appropriate staff of the Department of Legal
194 Affairs, the Department of Financial Services, and the
195 Department of Agriculture and Consumer Services to
196 participate in specified workgroups; authorizing such
197 staff to participate in specified workgroups and any
198 other workgroups as authorized by their respective
199 elected official; creating s. 282.0063, F.S.;
200 requiring DIGIT to perform specified actions to
201 develop and manage career paths, progressions, and
202 training programs for the benefit of state agency
203 personnel; requiring DIGIT to consult with specified

31-01058B-26

2026480

204 entities to implement specified provisions; creating
205 s. 282.0064, F.S.; requiring DIGIT, in coordination
206 with the Department of Management Services, to
207 establish a policy for all information technology-
208 related solicitations, contracts, and procurements;
209 specifying requirements for the policy related to
210 state term contracts, all contracts, and information
211 technology projects that require oversight;
212 prohibiting entities providing independent
213 verification and validation from having certain
214 interests, responsibilities, or other participation in
215 the project; providing the primary objective of
216 independent verification and validation; requiring the
217 entity performing such verification and validation to
218 provide specified regular reports and assessments;
219 requiring the Division of State Purchasing within the
220 Department of Management Services to coordinate with
221 DIGIT on state term contract solicitations and
222 invitations to negotiate; requiring DIGIT to evaluate
223 vendor responses and assist with answers to vendor
224 questions on such solicitations and invitations;
225 authorizing the Department of Legal Affairs, the
226 Department of Financial Services, and the Department
227 of Agriculture and Consumer Services to adopt
228 alternative information technology policy; providing
229 requirements for adopting such alternative policy;
230 amending s. 282.318, F.S.; providing that DIGIT is the
231 lead entity responsible for establishing enterprise
232 technology and cybersecurity standards and processes

31-01058B-26

2026480

233 and security measures that comply with specified
234 standards; requiring DIGIT to adopt specified rules;
235 requiring DIGIT to take specified actions; revising
236 the responsibilities of the state chief information
237 security officer; requiring state agencies to report
238 all ransomware incidents to the state chief
239 information security officer instead of the
240 Cybersecurity Operations Center; requiring state
241 agencies to also notify the Northwest Regional Data
242 Center of such incidents under specified conditions;
243 requiring the state chief information security
244 officer, instead of the Cybersecurity Operations
245 Center, to notify the Legislature of certain
246 incidents; requiring state agencies to notify the
247 state chief information security officer within
248 specified timeframes after the discovery of a
249 specified cybersecurity incident or ransomware
250 incident; requiring state agencies to also notify the
251 Northwest Regional Data Center of such incidents under
252 specified conditions; requiring the state chief
253 information security officer, instead of the
254 Cybersecurity Operations Center, to provide a certain
255 report on a quarterly basis to the Legislature;
256 revising the actions that state agency heads are
257 required to perform relating to cybersecurity;
258 revising the timeframe that the state agency strategic
259 cybersecurity plan must cover; requiring that a
260 specified comprehensive risk assessment be completed
261 biennially; specifying requirements for such

31-01058B-26

2026480

262 assessment; providing that confidential and exempt
263 records be made available to the state chief
264 information security officer and Legislature;
265 conforming provisions to changes made by the act;
266 amending s. 282.3185, F.S.; requiring the state chief
267 information security officer to perform specified
268 actions relating to cybersecurity training for state
269 employees; deleting obsolete language; requiring local
270 governments to notify the state chief information
271 security officer of compliance with specified
272 provisions as soon as possible; requiring local
273 governments to notify the state chief information
274 security officer, instead of the Cybersecurity
275 Operations Center, of cybersecurity or ransomware
276 incidents; revising the timeframes in which such
277 notifications must be made; requiring the state chief
278 information security officer to notify the Governor
279 and the Legislature of certain incidents within a
280 specified timeframe; authorizing local governments to
281 report certain cybersecurity incidents to the state
282 chief information security officer instead of the
283 Cybersecurity Operations Center; requiring the state
284 chief information security officer to provide a
285 certain consolidated incident report within a
286 specified timeframe to the Legislature; requiring the
287 state chief information security officer to establish
288 certain guidelines and processes by a specified date;
289 conforming provisions to changes made by the act;
290 conforming cross-references; repealing s. 282.319,

31-01058B-26

2026480

291 F.S., relating to the Florida Cybersecurity Advisory
292 Council; amending s. 282.201, F.S.; establishing the
293 state data center within the Northwest Regional Data
294 Center; requiring the Northwest Regional Data Center
295 to meet or exceed specified information technology
296 standards; revising requirements of the state data
297 center; abrogating the scheduled repeal of the
298 Division of Emergency Management's exemption from
299 using the state data center; deleting the Department
300 of Management Services' responsibilities related to
301 the state data center; deleting provisions relating to
302 contracting with the Northwest Regional Data Center;
303 creating s. 282.2011, F.S.; designating the Northwest
304 Regional Data Center as the state data center for all
305 state agencies; requiring the data center to engage in
306 specified actions; prohibiting state agencies from
307 terminating services with the data center without
308 giving written notice within a specified timeframe,
309 procuring third-party cloud-computing services without
310 evaluating the data center's cloud-computing services,
311 and exceeding a specified timeframe to remit payments
312 for services provided by the data center; specifying
313 circumstances under which the data center's
314 authorization to provide services may be terminated;
315 providing that the data center has a specified
316 timeframe to provide for the transition of state
317 agency customers to a qualified alternative cloud-
318 based data center that meets specified standards;
319 providing that the data center is the lead entity

31-01058B-26

2026480

320 responsible for creating, operating, and managing the
321 Florida Behavioral Health Care Data Repository;
322 providing the purpose of the repository; requiring the
323 data center, in collaboration with the Data Analysis
324 Committee of the Commission on Mental Health and
325 Substance Use Disorder, to develop a specified plan;
326 requiring, beginning on a specified date, the data
327 center to submit a certain report annually to the
328 Governor and the Legislature; providing for a
329 transition to an alternative cloud-based data center
330 under specified circumstances; amending s. 282.206,
331 F.S.; requiring state agencies to submit a certain
332 strategic plan to DIGIT and the Northwest Regional
333 Data Center annually by a specified date; amending s.
334 1004.649, F.S.; creating the Northwest Regional Data
335 Center at Florida State University; conforming
336 provisions to changes made by the act; amending s.
337 20.22, F.S.; conforming provisions to changes made by
338 the act; amending s. 282.802, F.S.; providing that the
339 Government Technology Modernization Council is located
340 within DIGIT; providing that the state chief
341 information officer, rather than the Secretary of
342 Management Services, is the ex officio head of the
343 council; requiring the council to submit a certain
344 recommendation to the Governor, the Commissioner of
345 Agriculture, the Chief Financial Officer, the Attorney
346 General, and the Legislature; conforming a cross-
347 reference; amending s. 282.604, F.S.; conforming
348 provisions to changes made by the act; amending s.

31-01058B-26

2026480

349 287.0591, F.S.; requiring the state chief information
350 officer, rather than the Florida Digital Service, to
351 participate in certain solicitations; amending s.
352 443.1113, F.S.; conforming provisions to changes made
353 by the act; amending s. 943.0415, F.S.; requiring the
354 state chief information security officer, rather than
355 the Florida Digital Service, to consult with the
356 Department of Law Enforcement's Cybercrime Office in
357 the adoption of certain rules; amending s. 1004.444,
358 F.S.; revising the list of who may request certain
359 assistance from the Florida Center for Cybersecurity;
360 providing an effective date.

361
362 Be It Enacted by the Legislature of the State of Florida:

364 Section 1. All duties, functions, records, pending issues,
365 existing contracts, administrative authority, and administrative
366 rules relating to the Florida Digital Service are transferred by
367 a type two transfer, as described in s. 20.06, Florida Statutes,
368 to the Division of Integrated Government Innovation and
369 Technology as created by this act. Any unexpended balances of
370 appropriations, allocations, and other public funds will revert
371 or will be appropriated or allocated as provided in the General
372 Appropriations Act or otherwise by law.

373 Section 2. Section 14.205, Florida Statutes, is created to
374 read:

375 14.205 Division of Integrated Government Innovation and
376 Technology.—

377 (1) Division of Integrated Government Innovation and

31-01058B-26

2026480

378 Technology is established within the Executive Office of the
379 Governor. The division shall be a separate budget entity, as
380 provided in the General Appropriations Act, and shall prepare
381 and submit a budget request in accordance with chapter 216. The
382 division shall be responsible for all professional, technical,
383 and administrative support functions necessary to carry out its
384 responsibilities under chapter 282 and as otherwise provided in
385 law.

386 (2) (a) The director of the division shall serve as the
387 state chief information officer. The director shall be appointed
388 by the Governor, subject to confirmation by the Senate. The
389 state chief information officer is prohibited from having any
390 financial, personal, or business conflicts of interest related
391 to technology vendors, contractors, or other information
392 technology service providers doing business with the state.

393 (b) The state chief information officer must meet the
394 following qualifications:

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

397 a. Hold a bachelor's degree from an accredited institution
398 in information technology, computer science, business
399 administration, public administration, or a related field; or
400 b. Hold a master's degree in any of the fields listed
401 above, which may be substituted for a portion of the experience
402 requirement.

403 2. Professional experience requirements.—The state chief
404 information officer must have at least 10 years of progressively
405 responsible experience in information technology management,
406 digital transformation, cybersecurity, or information technology

31-01058B-26

2026480

407 governance, including:

408 a. A minimum of 5 years in an executive or senior
409 leadership role, overseeing information technology strategy,
410 operations, or enterprise technology management, in either the
411 public or private sector;

412 b. Managing large-scale information technology projects,
413 enterprise infrastructure, and implementation of emerging
414 technologies;

415 c. Budget planning, procurement oversight, and financial
416 management of information technology investments; and

417 d. Working with state and federal information technology
418 regulations, digital services, and cybersecurity compliance
419 frameworks.

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

422 a. Cybersecurity and data protection by demonstrating
423 knowledge of cybersecurity risk management, compliance with
424 National Institute of Standards and Technology Cybersecurity
425 Framework, ISO 27001, and applicable federal and state security
426 regulations;

427 b. Cloud and digital services with experience with cloud
428 computing, enterprise systems modernization, digital
429 transformation, and emerging information technology trends;

430 c. Information technology governance and policy development
431 by demonstrating an understanding of statewide information
432 technology governance structures, digital services, and
433 information technology procurement policies; and

434 d. Public sector information technology management by
435 demonstrating familiarity with government information technology

31-01058B-26

2026480

436 funding models, procurement requirements, and legislative
437 processes affecting information technology strategy.

438 4. Leadership and administrative competencies.—The state
439 chief information officer must demonstrate:

440 a. Strategic vision and innovation by possessing the
441 capability to modernize information technology systems, drive
442 digital transformation, and align information technology
443 initiatives with state goals;

444 b. Collaboration and engagement with stakeholders by
445 working with legislators, state agency heads, local governments,
446 and private sector partners to implement information technology
447 initiatives;

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

451 d. Fiscal management and budget expertise managing multi-
452 million-dollar information technology budgets, cost-control
453 strategies, and financial oversight of information technology
454 projects.

455 (3) The deputy director of the division shall serve as the
456 deputy chief information officer. There also shall be selected
457 by the director separate positions for the state chief
458 information security officer and state chief data officer.

459 Section 3. Until a state chief information officer is
460 appointed pursuant to s. 14.205, Florida Statutes, the current
461 state chief information officer of the Department of Management
462 Services shall be transferred to the Division of Integrated
463 Government Innovation and Technology and serve as interim state
464 chief information officer. A state chief information officer for

31-01058B-26

2026480

465 the Division of Integrated Government Innovation and Technology
466 must be appointed by the Governor by June 30, 2027.

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

469 20.055 Agency inspectors general.—

470 (6) In carrying out the auditing duties and
471 responsibilities of this act, each inspector general shall
472 review and evaluate internal controls necessary to ensure the
473 fiscal accountability of the state agency. The inspector general
474 shall conduct financial, compliance, electronic data processing,
475 and performance audits of the agency and prepare audit reports
476 of his or her findings. The scope and assignment of the audits
477 are shall be determined by the inspector general; however, the
478 agency head may at any time request the inspector general to
479 perform an audit of a special program, function, or
480 organizational unit. In addition to these duties, each inspector
481 general annually shall review and evaluate the agency's
482 compliance with information technology reporting requirements
483 and the standards published by the Division of Integrated
484 Government Innovation and Technology. The inspector general
485 shall prepare an annual agency information technology compliance
486 report that assesses the adequacy of internal controls,
487 documentation, and implementation processes to ensure conformity
488 with statewide information technology governance, security, and
489 performance standards. The performance of the audits is audit
490 shall be under the direction of the inspector general, except
491 that if the inspector general does not possess the
492 qualifications specified in subsection (4), the director of
493 auditing must shall perform the functions listed in this

31-01058B-26

2026480

494 subsection.

495 (a) Such audits must ~~shall~~ be conducted in accordance with
496 the current International Standards for the Professional
497 Practice of Internal Auditing as published by the Institute of
498 Internal Auditors, Inc., or, where appropriate, in accordance
499 with generally accepted governmental auditing standards. All
500 audit reports issued by internal audit staff must ~~shall~~ include
501 a statement that the audit was conducted pursuant to the
502 appropriate standards.503 (b) Audit workpapers and reports are ~~shall be~~ public
504 records to the extent that they do not include information which
505 has been made confidential and exempt from the provisions of s.
506 119.07(1) pursuant to law. However, when the inspector general
507 or a member of the staff receives from an individual a complaint
508 or information that falls within the definition provided in s.
509 112.3187(5), the name or identity of the individual may not be
510 disclosed to anyone else without the written consent of the
511 individual, unless the inspector general determines that such
512 disclosure is unavoidable during the course of the audit or
513 investigation.514 (c) The inspector general and the staff shall have access
515 to any records, data, and other information of the state agency
516 he or she deems necessary to carry out his or her duties. The
517 inspector general may also request such information or
518 assistance as may be necessary from the state agency or from any
519 federal, state, or local government entity.520 (d) At the conclusion of each audit, the inspector general
521 shall submit preliminary findings and recommendations to the
522 person responsible for supervision of the program function or

31-01058B-26

2026480

523 operational unit who shall respond to any adverse findings
524 within 20 working days after receipt of the preliminary
525 findings. Such response and the inspector general's rebuttal to
526 the response must ~~shall~~ be included in the final audit report.

527 (e) At the conclusion of an audit in which the subject of
528 the audit is a specific entity contracting with the state or an
529 individual substantially affected, if the audit is not
530 confidential or otherwise exempt from disclosure by law, the
531 inspector general must ~~shall~~, consistent with s. 119.07(1),
532 submit the findings to the entity contracting with the state or
533 the individual substantially affected, who must ~~shall~~ be advised
534 in writing that they may submit a written response within 20
535 working days after receipt of the findings. The response and the
536 inspector general's rebuttal to the response, if any, must be
537 included in the final audit report.

538 (f) The inspector general shall submit the final report to
539 the agency head, the Auditor General, and, for state agencies
540 under the jurisdiction of the Governor, the Chief Inspector
541 General.

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

546 2. The Chief Inspector General shall review the annual
547 agency information technology compliance reports submitted by
548 agency inspectors general under the jurisdiction of the Governor
549 and shall prepare a consolidated statewide information
550 technology compliance report summarizing agency performance,
551 findings, and recommendations for improvement. The consolidated

31-01058B-26

2026480

552 report must be submitted to the Executive Office of the
553 Governor, the President of the Senate, and the Speaker of the
554 House of Representatives by December 1 of each year.

555 3. Agency heads for agencies not under the jurisdiction of
556 the Governor shall submit the annual agency information
557 technology compliance reports to the Executive Office of the
558 Governor, the President of the Senate, and the Speaker of the
559 House of Representatives by December 1 of each year.

560 (g) The Auditor General, in connection with the independent
561 postaudit of the same agency pursuant to s. 11.45, shall give
562 appropriate consideration to internal audit reports and the
563 resolution of findings therein. The Legislative Auditing
564 Committee may inquire into the reasons or justifications for
565 failure of the agency head to correct the deficiencies reported
566 in internal audits that are also reported by the Auditor General
567 and shall take appropriate action.

568 (h) The inspector general shall monitor the implementation
569 of the state agency's response to any report on the state agency
570 issued by the Auditor General or by the Office of Program Policy
571 Analysis and Government Accountability. No later than 6 months
572 after the Auditor General or the Office of Program Policy
573 Analysis and Government Accountability publishes a report on the
574 state agency, the inspector general shall provide a written
575 response to the agency head or, for state agencies under the
576 jurisdiction of the Governor, the Chief Inspector General on the
577 status of corrective actions taken. The inspector general shall
578 file a copy of such response with the Legislative Auditing
579 Committee.

580 (i) The inspector general shall develop long-term and

31-01058B-26

2026480

581 annual audit plans based on the findings of periodic risk
582 assessments. The plan, where appropriate, should include
583 postaudit samplings of payments and accounts. The plan must
584 ~~shall~~ show the individual audits to be conducted during each
585 year and related resources to be devoted to the respective
586 audits. The plan must ~~shall~~ include a specific cybersecurity
587 audit plan. The Chief Financial Officer, to assist in fulfilling
588 the responsibilities for examining, auditing, and settling
589 accounts, claims, and demands pursuant to s. 17.03(1), and
590 examining, auditing, adjusting, and settling accounts pursuant
591 to s. 17.04, may use audits performed by the inspectors general
592 and internal auditors. For state agencies under the jurisdiction
593 of the Governor, the audit plans must ~~shall~~ be submitted to the
594 Chief Inspector General. The plan must ~~shall~~ be submitted to the
595 agency head for approval. A copy of the approved plan must ~~shall~~
596 be submitted to the Auditor General.

597 Section 5. Paragraph (b) of subsection (3) of section
598 97.0525, Florida Statutes, is amended to read:

599 97.0525 Online voter registration.—

600 (3)

601 (b) The division shall conduct a comprehensive risk
602 assessment of the online voter registration system every 2
603 years. The comprehensive risk assessment must comply with the
604 risk assessment methodology developed by the Division of
605 Integrated Government Innovation and Technology Department of
606 ~~Management Services~~ for identifying security risks, determining
607 the magnitude of such risks, and identifying areas that require
608 safeguards. In addition, the comprehensive risk assessment must
609 incorporate all of the following:

31-01058B-26

2026480

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

615 2. Screening of computers and networks used to support the
616 online voter registration system for malware and other
617 vulnerabilities.

618 3. Evaluation of database infrastructure, including
619 software and operating systems, in order to fortify defenses
620 against cyberattacks.

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

624 Section 6. Paragraphs (a) and (f) of subsection (1),
625 paragraphs (b) and (c) of subsection (2), and subsections (3)
626 and (4) of section 112.22, Florida Statutes, are amended to
627 read:

628 112.22 Use of applications from foreign countries of
629 concern prohibited.—

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

631 (a) DIGIT means the Division of Integrated Government
632 Innovation and Technology ~~Department~~ means the Department of
633 ~~Management Services~~.

634 (f) "Prohibited application" means an application that
635 meets the following criteria:

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

31-01058B-26

2026480

639 a. Collecting keystrokes or sensitive personal, financial,
640 proprietary, or other business data;

641 b. Compromising e-mail and acting as a vector for
642 ransomware deployment;

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

644 d. Conducting surveillance and tracking of individual
645 users; or

646 e. Using algorithmic modifications to conduct
647 disinformation or misinformation campaigns; or

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

652 (2)

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

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

660 2. A public employer may request a waiver from DIGIT the
661 department to allow designated employees or officers to download
662 or access a prohibited application on a government-issued
663 device.

664 (c) Within 15 calendar days after DIGIT the department
665 issues or updates its list of prohibited applications pursuant
666 to paragraph (3)(a), an employee or officer of a public employer
667 who uses a government-issued device must remove, delete, or

31-01058B-26

2026480

668 uninstall any prohibited applications from his or her
669 government-issued device.

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

671 (a) Compile and maintain a list of prohibited applications
672 and publish the list on its website. DIGIT The department shall
673 update this list quarterly and shall provide notice of any
674 update to public employers.

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

678 1. A description of the activity to be conducted and the
679 state interest furthered by the activity.

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

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

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

689 5. A description of the circumstances under which the
690 waiver applies.

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

696 (b) DIGIT The department shall adopt rules necessary to

31-01058B-26

2026480

697 administer this section.

698 Section 7. Paragraph (a) of subsection (5) of section
699 119.0725, Florida Statutes, is amended to read:

700 119.0725 Agency cybersecurity information; public records
701 exemption; public meetings exemption.—

702 (5) (a) Information made confidential and exempt pursuant to
703 this section must ~~shall~~ be made available to a law enforcement
704 agency, the Auditor General, the Cybercrime Office of the
705 Department of Law Enforcement, the Division of Integrated
706 Government Innovation and Technology ~~Florida Digital Service~~
707 ~~within the Department of Management Services~~, and, for agencies
708 under the jurisdiction of the Governor, the Chief Inspector
709 General.

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

712 216.023 Legislative budget requests to be furnished to
713 Legislature by agencies.—

714 (4) (a) The legislative budget request for each program must
715 contain:

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

718 2. Information on expenditures for 3 fiscal years (actual
719 prior-year expenditures, current-year estimated expenditures,
720 and agency budget requested expenditures for the next fiscal
721 year) by appropriation category.

722 3. Details on trust funds and fees.

723 4. The total number of positions (authorized, fixed, and
724 requested).

725 5. An issue narrative describing and justifying changes in

31-01058B-26

2026480

726 amounts and positions requested for current and proposed
727 programs for the next fiscal year.

728 6. Information resource requests.

729 7. Supporting information, including applicable cost-
730 benefit analyses, business case analyses, performance
731 contracting procedures, service comparisons, and impacts on
732 performance standards for any request to outsource or privatize
733 agency functions. The cost-benefit and business case analyses
734 must include an assessment of the impact on each affected
735 activity from those identified in accordance with paragraph (b).
736 Performance standards must include standards for each affected
737 activity and be expressed in terms of the associated unit of
738 activity.

739 8. An evaluation of major outsourcing and privatization
740 initiatives undertaken during the last 5 fiscal years having
741 aggregate expenditures exceeding \$10 million during the term of
742 the contract. The evaluation must include an assessment of
743 contractor performance, a comparison of anticipated service
744 levels to actual service levels, and a comparison of estimated
745 savings to actual savings achieved. Consolidated reports issued
746 by the Department of Management Services may be used to satisfy
747 this requirement.

748 9. Supporting information for any proposed consolidated
749 financing of deferred-payment commodity contracts including
750 guaranteed energy performance savings contracts. Supporting
751 information must also include narrative describing and
752 justifying the need, baseline for current costs, estimated cost
753 savings, projected equipment purchases, estimated contract
754 costs, and return on investment calculation.

31-01058B-26

2026480

755 10. For projects that exceed \$10 million in total cost, the
756 statutory reference of the existing policy or the proposed
757 substantive policy that establishes and defines the project's
758 governance structure, planned scope, main business objectives
759 that must be achieved, and estimated completion timeframes. The
760 governance structure for information technology-related projects
761 must incorporate the applicable project management and oversight
762 standards established pursuant to s. 282.0061 ~~s. 282.0051~~.
763 Information technology budget requests for the continuance of
764 existing hardware and software maintenance agreements, renewal
765 of existing software licensing agreements, or the replacement of
766 desktop units with new technology that is similar to the
767 technology currently in use are exempt from this requirement.

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

774 ~~(a) The name of the technology system.~~
775 ~~(b) A brief description of the purpose and function of the
776 system.~~
777 ~~(c) A brief description of the goals of the project.~~
778 ~~(d) The initiation date of the project.~~
779 ~~(e) The key performance indicators for the project.~~
780 ~~(f) Any other metrics for the project evaluating the health
781 and status of the project.~~
782 ~~(g) The original and current baseline estimated end dates
783 of the project.~~

31-01058B-26

2026480

(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 (2) through (11) and (36), (37), and (38) of section 282.0041, Florida Statutes, are redesignated as subsections (1) through (10) and (37), (38), and (39), respectively, new subsections (11) and (36) are added to that section, and present subsections (1) and (7) 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 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.

31-01058B-26

2026480

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

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

821 282.00515 Duties of Cabinet agencies.—

822 (1) (a) The Department of Legal Affairs, the Department of
823 Financial Services, and the Department of Agriculture and
824 Consumer Services shall adopt the standards, best practices,
825 processes, and methodologies established in s. 282.0061(4) and
826 (5) (b) and (d). However, such departments may s. 282.0051(1)(b),
827 (e), and (r) and (3) (e) or adopt alternative standards, best
828 practices, and methodologies that must be based on best
829 practices and industry standards that allow for open data
830 interoperability. Such departments shall evaluate the adoption
831 of alternative standards on a case-by-case basis for each
832 standard, project, or system and reevaluate such alternative
833 standards periodically.

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

31-01058B-26

2026480

842 (2) If the Department of Legal Affairs, the Department of
843 Financial Services, or the Department of Agriculture and
844 Consumer Services adopts alternative standards, best practices,
845 processes, and methodologies in lieu of the enterprise
846 architecture standards, best practices, processes, and
847 methodologies adopted pursuant to s. 282.0061(4) and (5)(b) and
848 (d) s. 282.0051, such department must notify DIGIT, the
849 Governor, the President of the Senate, and the Speaker of the
850 House of Representatives in writing of the adoption of the
851 alternative standards and provide a justification for adoption
852 of the alternative standards and explain the manner in which how
853 the agency will achieve the policy, standard, guideline, or best
854 practice open data interoperability.

855 (3) The Department of Legal Affairs, the Department of
856 Financial Services, and the Department of Agriculture and
857 Consumer Services shall each conduct a full baseline needs
858 assessment to document their respective technical environments,
859 existing technical debt, security risks, and compliance with
860 adopted information technology best practices, guidelines, and
861 standards, similar to the assessments conducted by DIGIT
862 pursuant to s. 282.0061(2)(a) and (b). The Department of Legal
863 Affairs, the Department of Financial Services, and the
864 Department of Agriculture and Consumer Services may contract
865 with DIGIT to assist with or complete the assessments.

866 (4) The Department of Legal Affairs, the Department of
867 Financial Services, and the Department of Agriculture and
868 Consumer Services shall each produce a phased roadmap for
869 strategic planning to address known technology gaps and
870 deficiencies, similar to the assessments conducted by DIGIT

31-01058B-26

2026480

871 pursuant to s. 282.0061(2) (d). The phased roadmap must be
872 submitted annually with legislative budget requests required
873 under s. 216.023. The Department of Legal Affairs, the
874 Department of Financial Services, and the Department of
875 Agriculture and Consumer Services may contract with DIGIT to
876 assist with or complete the phased roadmap.

877 (5) The Department of Legal Affairs, the Department of
878 Financial Services, and the Department of Agriculture and
879 Consumer Services may, but are not required to, contract with
880 DIGIT the department to provide procurement advisory and review
881 services for information technology projects as provided in s.
882 282.0061(5) (a) or perform any of the services and functions
883 described in s. 282.0051.

884 (6) The Department of Legal Affairs, the Department of
885 Financial Services, and the Department of Agriculture and
886 Consumer Services shall use the information technology reports
887 developed by DIGIT pursuant to s. 282.0061(5) (e) and follow the
888 streamlined reporting process pursuant to s. 282.0061(5) (h). The
889 Department of Legal Affairs, the Department of Financial
890 Services, and the Department of Agriculture and Consumer
891 Services shall report annually to the President of the Senate
892 and the Speaker of the House of Representatives by December 15
893 information related to the respective department similar to the
894 information required under s. 282.006(6) (a) and the information
895 technology financial data methodology and reporting required by
896 s. 282.0061(6). The Department of Legal Affairs, the Department
897 of Financial Services, and the Department of Agriculture and
898 Consumer Services may provide the report required under this
899 subsection collectively with DIGIT or shall report separately to

31-01058B-26

2026480

900 the Governor, the President of the Senate, and the Speaker of
901 the House of Representatives.

902 (7) (a) ~~(4) (a)~~ Nothing in this chapter section or in s.
903 ~~282.0051~~ requires the Department of Legal Affairs, the
904 Department of Financial Services, or the Department of
905 Agriculture and Consumer Services to integrate with information
906 technology outside its own department or with DIGIT the Florida
907 Digital Service.

908 (b) ~~DIGIT The department, acting through the Florida~~
909 ~~Digital Service,~~ may not retrieve or disclose any data without a
910 shared-data agreement in place between DIGIT the department and
911 the Department of Legal Affairs, the Department of Financial
912 Services, or the Department of Agriculture and Consumer
913 Services.

914 (8) Notwithstanding s. 282.0061(5)(g), DIGIT may perform
915 project oversight only on information technology projects of the
916 Department of Legal Affairs, the Department of Financial
917 Services, and the Department of Agriculture and Consumer
918 Services which have a project cost of \$20 million or more. Such
919 information technology projects must also comply with the
920 applicable information technology architecture, project
921 management and oversight, and reporting standards established by
922 DIGIT. DIGIT shall report by the 30th day after the end of each
923 quarter to the President of the Senate and the Speaker of the
924 House of Representatives on any information technology project
925 under this subsection which DIGIT identifies as high risk. The
926 report must include a risk assessment, including fiscal risks,
927 associated with proceeding to the next stage of the project, and
928 a recommendation for any corrective action required, including

31-01058B-26

2026480

929 suspension or termination of the project.

930 (9) If an information technology project implemented by a
931 state agency must be connected to or otherwise accommodated by
932 an information technology system administered by the Department
933 of Legal Affairs, the Department of Financial Services, or the
934 Department of Agriculture and Consumer Services, DIGIT must
935 consult with the applicable department regarding the risks and
936 other effects of such project on the department's information
937 technology systems and must work cooperatively with the
938 department regarding connections, interfaces, timing, or
939 accommodations required to implement such project.

940 Section 11. Section 282.006, Florida Statutes, is created
941 to read:

942 282.006 Division of Integrated Government Innovation and
943 Technology; enterprise responsibilities; reporting.—

944 (1) The Division of Integrated Government Innovation and
945 Technology established in s. 14.205 is the state organization
946 for information technology governance and is the lead entity
947 responsible for understanding the unique state agency
948 information technology needs and environments, creating
949 technology standards and strategy, supporting state agency
950 technology efforts, and reporting on the status of technology
951 for state agencies.

952 (2) The Legislature intends for DIGIT policy, standards,
953 guidance, and oversight to allow for adaptability to emerging
954 technology and organizational needs while maintaining compliance
955 with industry best practices. All policies, standards, and
956 guidelines established pursuant to this chapter must be
957 technology-agnostic and may not prescribe specific tools,

31-01058B-26

2026480

958 platforms, or vendors.

959 (3) DIGIT shall establish the strategic direction of
960 information technology for state agencies. DIGIT shall develop
961 and publish information technology policy that aligns with
962 industry best practices for the management of the state's
963 information technology resources. The policy must be updated as
964 necessary to meet the requirements of this chapter and
965 advancements in technology.

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

969 (a) Acknowledges the unique needs of the entities within
970 the enterprise in the development and publication of standards
971 and terminologies to facilitate digital interoperability;

972 (b) Supports the cloud-first policy as specified in s.
973 282.206;

974 (c) Addresses the manner in which information technology
975 infrastructure may be modernized to achieve security,
976 scalability, maintainability, interoperability, and improved
977 cost-efficiency goals; and

978 (d) Includes, at a minimum, best practices, guidelines, and
979 standards for:

- 980 1. Data models and taxonomies.
- 981 2. Master data management.
- 982 3. Data integration and interoperability.
- 983 4. Data security and encryption.
- 984 5. Bot prevention and data protection.
- 985 6. Data backup and recovery.
- 986 7. Application portfolio and catalog requirements.

31-01058B-26

2026480

987 8. Application architectural patterns and principles.
988 9. Technology and platform standards.
989 10. Secure coding practices.
990 11. Performance and scalability.
991 12. Cloud infrastructure and architecture.
992 13. Networking, connectivity, and security protocols.
993 14. Authentication, authorization, and access controls.
994 15. Disaster recovery.
995 16. Quality assurance.
996 17. Testing methodologies and measurements.
997 18. Logging and log retention.
998 19. Application and use of artificial intelligence.
999 (5) DIGIT shall develop open data technical standards and
1000 terminologies for use by state agencies. DIGIT shall develop
1001 enterprise technology testing and quality assurance best
1002 practices and standards to ensure the reliability, security, and
1003 performance of information technology systems. Such best
1004 practices and standards must include:
1005 (a) Functional testing to ensure software or systems meet
1006 required specifications.
1007 (b) Performance and load testing to ensure software and
1008 systems operate efficiently under various conditions.
1009 (c) Security testing to protect software and systems from
1010 vulnerabilities and cyber threats.
1011 (d) Compatibility and interoperability testing to ensure
1012 software and systems operate seamlessly across environments.
1013 (6) DIGIT shall produce and provide the following reports
1014 to the Governor, the President of the Senate, and the Speaker of
1015 the House of Representatives:

31-01058B-26

2026480

1016 (a) Annually by December 15, an enterprise analysis report
1017 for state agencies that includes all of the following:
1018 1. Results of the state agency needs assessments, including
1019 any plan to address technical debt as required by s. 282.0061
1020 pursuant to the schedule adopted.
1021 2. Alternative standards related to federal funding adopted
1022 pursuant to s. 282.0061.
1023 3. Information technology financial data for each state
1024 agency for the previous fiscal year. This portion of the annual
1025 report must include, at a minimum, the following recurring and
1026 nonrecurring information:
1027 a. Total number of full-time equivalent positions.
1028 b. Total amount of salary.
1029 c. Total amount of benefits.
1030 d. Total number of comparable full-time equivalent
1031 positions and total amount of expenditures for information
1032 technology staff augmentation.
1033 e. Total number of contracts and purchase orders and total
1034 amount of associated expenditures for information technology
1035 managed services.
1036 f. Total amount of expenditures by state term contract as
1037 defined in s. 287.012, contracts procured using alternative
1038 purchasing methods as authorized pursuant to s. 287.042(16), and
1039 state agency procurements through request for proposal,
1040 invitation to negotiate, invitation to bid, single source, and
1041 emergency purchases.
1042 g. Total amount of expenditures for hardware.
1043 h. Total amount of expenditures for non-cloud software.
1044 i. Total amount of expenditures for cloud software licenses

31-01058B-26

2026480

1045 and services with a separate amount for expenditures for state
1046 data center services.

1047 j. Total amount of expenditures for cloud data center
1048 services with a separate amount for expenditures for state data
1049 center services.

1050 k. Total amount of expenditures for administrative costs.

1051 4. Consolidated information for the previous fiscal year
1052 about state information technology projects, which must include,
1053 at a minimum, the following information:

1054 a. Anticipated funding requirements for information
1055 technology support over the next 5 years.

1056 b. An inventory of current information technology assets
1057 and major projects. As used in this paragraph, the term "major
1058 project" includes projects costing more than \$500,000 to
1059 implement.

1060 c. Significant unmet needs for information technology
1061 resources over the next 5 fiscal years, ranked in priority order
1062 according to their urgency.

1063 5. A review and summary of whether the information
1064 technology contract policy established pursuant to s. 282.0064
1065 is included in all solicitations and contracts.

1066 (b) Biennially by December 15 of even-numbered years, a
1067 report on the strategic direction of information technology in
1068 the state which includes recommendations for all of the
1069 following:

1070 1. Standardization and consolidation of information
1071 technology services that are identified as common across state
1072 agencies as required in s. 282.0061.

1073 2. Information technology services needed to be designed,

31-01058B-26

2026480

1074 delivered, and managed as state agency enterprise information
1075 technology services. Recommendations must include the
1076 identification of existing information technology resources
1077 associated with the services, if existing services must be
1078 transferred as a result of being delivered and managed as
1079 enterprise information technology services, and which entity is
1080 best suited to manage the service.

1081 (c)1. When conducted as provided in this paragraph, a
1082 market analysis and accompanying strategic plan submitted by
1083 December 31 of each year that the market analysis is conducted.

1084 2. No less frequently than every 3 years, DIGIT shall
1085 conduct market analysis to determine whether the:

1086 a. Information technology resources across state agencies
1087 are used in the most cost-effective and cost-efficient manner,
1088 while recognizing that the replacement of certain legacy
1089 information technology systems within the enterprise may be cost
1090 prohibitive or cost inefficient due to the remaining useful life
1091 of those resources; and

1092 b. State agencies are using best practices with respect to
1093 information technology, information services, and the
1094 acquisition of emerging technologies and information services.

1095 3. Each market analysis must be used to prepare a strategic
1096 plan for continued and future information technology and
1097 information services, including, but not limited to, proposed
1098 acquisition of new services or technologies and approaches to
1099 the implementation of any new services or technologies.

1100 (6) (a) DIGIT shall develop, implement, and maintain a
1101 library to serve as the official repository for all enterprise
1102 information technology policies, standards, guidelines, and best

31-01058B-26

2026480

1103 practices applicable to state agencies. The online library must
1104 be accessible and searchable by all state agencies and the
1105 Department of Legal Affairs, the Department of Financial
1106 Services, and the Department of Agriculture and Consumer
1107 Services, through a secure authentication system. The library
1108 must include standardized checklists organized by technical
1109 subject areas to assist state agencies in measuring compliance
1110 with the information technology policies, standards, guidelines,
1111 and best practices.

1112 (b) DIGIT shall establish procedures to ensure the
1113 integrity, security, and availability of the library, including
1114 appropriate access controls, encryption, and disaster recovery
1115 measures. DIGIT shall regularly update documents and materials
1116 of the library to reflect current state and federal
1117 requirements, industry best practices, and emerging technologies
1118 and shall maintain version control and revision history for all
1119 published documents. DIGIT shall create mechanisms for state
1120 agencies to submit feedback, request clarifications, and
1121 recommend updates.

1122 (7) (a) Each state agency shall actively participate and
1123 collaborate with DIGIT to achieve the objectives set forth in
1124 this chapter. Each state agency shall also adhere to the
1125 policies, standards, guidelines, and best practices established
1126 by DIGIT in information technology planning, procurement,
1127 implementation, and operations as required by this chapter.

1128 (b) 1. A state agency may request an exemption to a specific
1129 policy, standard, or guideline when compliance is not
1130 technically feasible, would cause undue hardship, or conflicts
1131 with any agency-specific statutory requirement. The state agency

31-01058B-26

2026480

1132 requesting an exception must submit a formal justification to
1133 DIGIT detailing all of the following:

1134 a. The specific requirement for which an exemption is
1135 sought.

1136 b. The reason compliance is not feasible or practical.

1137 c. Any compensating control or alternative measure the
1138 state agency will implement to mitigate associated risks.

1139 d. The anticipated duration of the exemption.

1140 2. DIGIT shall review all exemption requests and provide a
1141 recommendation to the state chief information officer who shall
1142 present the compliance exemption requests to the chief
1143 information officer workgroup. Approval of exemption requests
1144 must be made by a majority vote of the workgroup. Approved
1145 exemptions must be documented, including conditions and
1146 expiration dates.

1147 3. A state agency with an approved exemption shall undergo
1148 periodic review to determine whether the exemption remains
1149 necessary or whether compliance can be achieved.

1150 (8) DIGIT may adopt rules to implement this chapter.

1151 Section 12. Section 282.0061, Florida Statutes, is created
1152 to read:

1153 282.0061 DIGIT support of state agencies; information
1154 technology procurement and projects.—

1155 (1) LEGISLATIVE INTENT.—The Legislature intends for DIGIT
1156 to support state agencies in their information technology
1157 efforts through the adoption of policies, standards, and
1158 guidance and by providing oversight that recognizes unique state
1159 agency information technology needs, environments, and goals.

1160 DIGIT assistance and support must allow for adaptability to

31-01058B-26

2026480

1161 emerging technologies and organizational needs while maintaining
1162 compliance with industry best practices. DIGIT may not prescribe
1163 specific tools, platforms, or vendors.

1164 (2) NEEDS ASSESSMENTS.—

1165 (a) By January 1, 2029, DIGIT shall conduct full baseline
1166 needs assessments of state agencies to document their respective
1167 technical environments, existing technical debt, security risks,
1168 and compliance with all information technology standards and
1169 guidelines developed and published by DIGIT. The needs
1170 assessment must use the latest version of the Capability
1171 Maturity Model Integration to evaluate each state agency's
1172 information technology capabilities, providing a maturity level
1173 rating for each assessed domain. After completion of the initial
1174 full baseline needs assessment, such assessments must be
1175 maintained and updated on a regular schedule adopted by DIGIT.

1176 (b) In assessing the existing technical debt portion of the
1177 needs assessment, DIGIT shall analyze the state's legacy
1178 information technology systems and develop a plan to document
1179 the needs and costs for replacement systems. The plan must
1180 include an inventory of legacy applications and infrastructure;
1181 the required capabilities not available with the legacy system;
1182 the estimated process, timeline, and cost to migrate from legacy
1183 environments; and any other information necessary for fiscal or
1184 technology planning. The plan must determine and document the
1185 estimated timeframe during which the state agency can continue
1186 to efficiently use legacy information technology systems,
1187 resources, security, and data management to support operations.
1188 State agencies shall provide all necessary documentation to
1189 enable accurate reporting on legacy systems.

31-01058B-26

2026480

1190 (c) DIGIT shall develop a plan and schedule to conduct the
1191 initial full baseline needs assessments. By October 1, 2027,
1192 DIGIT shall submit the plan to the Governor, the President of
1193 the Senate, and the Speaker of the House of Representatives.

1194 (d) DIGIT shall support state agency strategic planning
1195 efforts and assist state agencies with the production of a
1196 phased roadmap to address known technology gaps and deficiencies
1197 as identified in the needs assessments. The roadmaps must
1198 include specific strategies and initiatives aimed at advancing
1199 the state agency's maturity level in accordance with the latest
1200 version of the Capability Maturity Model Integration. State
1201 agencies shall create, maintain, and submit the roadmap on an
1202 annual basis with their legislative budget requests required
1203 under s. 216.023.

1204 (3) STANDARDIZATION.—DIGIT shall:

1205 (a) Recommend in its annual enterprise analysis report for
1206 state agencies required under s. 282.006 any potential method
1207 for standardizing data across state agencies which will promote
1208 interoperability and reduce the collection of duplicative data.

1209 (b) Identify any opportunities in such enterprise analysis
1210 report for state agencies for standardization and consolidation
1211 of information technology services that are common across all
1212 state agencies and that support:

1213 1. Improved interoperability, security, scalability,
1214 maintainability, and cost efficiency; and

1215 2. Business functions and operations, including
1216 administrative functions such as purchasing, accounting and
1217 reporting, cash management, and personnel.

1218 (4) DATA MANAGEMENT.—

31-01058B-26

2026480

1219 (a) DIGIT shall develop standards for use by state agencies
1220 which support best practices for master data management at the
1221 state agency level to facilitate enterprise data sharing and
1222 interoperability.

1223 (b) DIGIT shall establish a methodology and strategy for
1224 implementing statewide master data management and submit a
1225 report to the Governor, the President of the Senate, and the
1226 Speaker of the House of Representatives by December 1, 2029. The
1227 report must include the vision, goals, and benefits of
1228 implementing a statewide master data management initiative, an
1229 analysis of the current state of data management, and the
1230 recommended strategy, methodology, and estimated timeline and
1231 resources needed at a state agency and enterprise level to
1232 accomplish the initiative.

1233 (5) INFORMATION TECHNOLOGY PROJECTS.—DIGIT has the
1234 following duties and responsibilities related to state agency
1235 technology projects:

1236 (a) Provide procurement advisory and review services for
1237 information technology projects to all state agencies, including
1238 procurement and contract development assistance to meet the
1239 information technology contract policy established pursuant to
1240 s. 282.0064.

1241 (b) Establish best practices and procurement processes and
1242 develop metrics to support these processes for the procurement
1243 of information technology products and services in order to
1244 reduce costs or improve the provision of government services.

1245 (c) Upon request, assist state agencies in the development
1246 of information technology-related legislative budget requests.

1247 (d) Develop standards and accountability measures for

31-01058B-26

2026480

1248 information technology projects, including criteria for
1249 effective project management and oversight. State agencies shall
1250 satisfy these standards and measures when implementing
1251 information technology projects. To support data-driven decision
1252 making, the standards and measures must include, but are not
1253 limited to:

1254 1. Performance measurements and metrics that objectively
1255 reflect the status of an information technology project based on
1256 a defined and documented project scope, to include the volume of
1257 impacted stakeholders, cost, and schedule.

1258 2. Methodologies for calculating and defining acceptable
1259 variances in the projected versus actual scope, schedule, or
1260 cost of an information technology project.

1261 3. Reporting requirements designed to alert all defined
1262 stakeholders that an information technology project has exceeded
1263 acceptable variances defined and documented in a project plan as
1264 well as any variance that represents a schedule delay of 1 month
1265 or more or a cost increase of \$1 million or more.

1266 4. Technical standards to ensure an information technology
1267 project complies with the enterprise architecture standards.

1268 (e) Develop information technology project reports for use
1269 by state agencies, including, but not limited to, operational
1270 work plans, project spending plans, and project status reports.
1271 Reporting standards must include content, format, and frequency
1272 of project updates.

1273 (f) Provide training opportunities to state agencies to
1274 assist in the adoption of the project management and oversight
1275 standards.

1276 (g) Perform project oversight on all state agency

31-01058B-26

2026480

1277 information technology projects that have total project costs of
1278 \$10 million or more. DIGIT shall report by the 30th day after
1279 the end of each quarter to the Executive Office of the Governor,
1280 the President of the Senate, and the Speaker of the House of
1281 Representatives on any information technology project that DIGIT
1282 identifies as high-risk. The report must include a risk
1283 assessment, including fiscal risks, associated with proceeding
1284 to the next stage of the project, and a recommendation for
1285 corrective actions required, including suspension or termination
1286 of the project.

1287 (h) Establish a streamlined reporting process with clear
1288 timelines and escalation procedures for notifying a state agency
1289 of noncompliance with the standards developed and adopted by
1290 DIGIT.

1291 (6) INFORMATION TECHNOLOGY FINANCIAL DATA.—

1292 (a) In consultation with state agencies, DIGIT shall create
1293 a methodology, an approach, and applicable templates and formats
1294 for identifying and collecting both current and planned
1295 information technology expenditure data at the state agency
1296 level. DIGIT shall continuously obtain, review, and maintain
1297 records of the appropriations, expenditures, and revenues for
1298 information technology for each state agency.

1299 (b) DIGIT shall prescribe the format for state agencies to
1300 provide all necessary financial information to DIGIT for
1301 inclusion in the annual report required under s. 282.006. State
1302 agencies shall provide the information to DIGIT by October 1 for
1303 the previous fiscal year.

1304 (7) FEDERAL CONFLICTS.—DIGIT must work with state agencies
1305 to provide alternative standards, policies, or requirements that

31-01058B-26

2026480

1306 do not conflict with federal regulations or requirements if
1307 adherence to standards or policies adopted by or established
1308 pursuant to this section conflict with federal regulations or
1309 requirements imposed on an entity within the enterprise and
1310 results in, or is expected to result in, adverse action against
1311 any state agency or loss of federal funding.

1312 Section 13. Section 282.0062, Florida Statutes, is created
1313 to read:

1314 282.0062 DIGIT workgroups.—The following workgroups are
1315 established within DIGIT to facilitate coordination with state
1316 agencies:

1317 (1) CHIEF INFORMATION OFFICER WORKGROUP.—

1318 (a) The chief information officer workgroup, composed of
1319 all state agency chief information officers, shall consider and
1320 make recommendations to the state chief information officer and
1321 the state chief information architect on such matters as
1322 enterprise information technology policies, standards, services,
1323 and architecture. The workgroup may also identify and recommend
1324 opportunities for the establishment of public-private
1325 partnerships when considering technology infrastructure and
1326 services in order to accelerate project delivery and provide a
1327 source of new or increased project funding.

1328 (b) At a minimum, the state chief information officer shall
1329 consult with the workgroup on a quarterly basis with regard to
1330 executing the duties and responsibilities of the state agencies
1331 related to statewide information technology strategic planning
1332 and policy.

1333 (2) ENTERPRISE DATA AND INTEROPERABILITY WORKGROUP.—

1334 (a) The enterprise data and interoperability workgroup,

31-01058B-26

2026480

1335 composed of chief data officer representatives from all state
1336 agencies, shall consider and make recommendations to the state
1337 chief data officer on such matters as enterprise data policies,
1338 standards, services, and architecture that promote data
1339 consistency, accessibility, and seamless integration across the
1340 enterprise.

1341 (b) At a minimum, the state chief data officer shall
1342 consult with the workgroup on a quarterly basis with regard to
1343 executing the duties and responsibilities of the state agencies
1344 related to statewide data governance planning and policy.

1345 (3) ENTERPRISE SECURITY WORKGROUP.—
1346 (a) The enterprise security workgroup, composed of chief
1347 information security officer representatives from all state
1348 agencies, shall consider and make recommendations to the state
1349 chief information security officer on such matters as
1350 cybersecurity policies, standards, services, and architecture
1351 that promote the protection of state assets.

1352 (b) At a minimum, the state chief information security
1353 officer shall consult with the workgroup on a quarterly basis
1354 with regard to executing the duties and responsibilities of the
1355 state agencies related to cybersecurity governance and policy
1356 development.

1357 (4) ENTERPRISE INFORMATION TECHNOLOGY QUALITY ASSURANCE
1358 WORKGROUP.—

1359 (a) The enterprise information technology quality assurance
1360 workgroup, composed of testing and quality assurance
1361 representatives from all state agencies, shall consider and make
1362 recommendations to the state chief technology officer on such
1363 matters as testing methodologies, tools, and best practices to

31-01058B-26

2026480

1364 reduce risks related to software defects, cybersecurity threats,
1365 and operational failures.

1366 (b) At a minimum, the state chief information officer shall
1367 consult with the workgroup on a quarterly basis with regard to
1368 executing the duties and responsibilities of the state agencies
1369 related to enterprise software testing and quality assurance
1370 standards.

1371 (5) ENTERPRISE INFORMATION TECHNOLOGY PROJECT MANAGEMENT
1372 WORKGROUP.—

1373 (a) The enterprise information technology project
1374 management workgroup, composed of information technology project
1375 manager representatives from all state agencies, shall consider
1376 and make recommendations to the state chief technology officer
1377 on such matters as information technology project management
1378 policies, standards, accountability measures, and services that
1379 promote project governance and standardization across the
1380 enterprise.

1381 (b) At a minimum, the state chief information officer shall
1382 consult with the workgroup on a quarterly basis with regard to
1383 executing the duties and responsibilities of the state agencies
1384 related to project management and oversight.

1385 (6) ENTERPRISE INFORMATION TECHNOLOGY PURCHASING
1386 WORKGROUP.—

1387 (a) The enterprise information technology purchasing
1388 workgroup, composed of information technology procurement
1389 representatives from all state agencies, shall consider and make
1390 recommendations to the state chief information technology
1391 procurement officer on such matters as information technology
1392 procurement policies, standards, and purchasing strategy and

31-01058B-26

2026480

1393 optimization that promote best practices for contract
1394 negotiation, consolidation, and effective service-level
1395 agreement implementation across the enterprise.

1396 (b) At a minimum, the state chief information officer shall
1397 consult with the workgroup on a quarterly basis with regard to
1398 executing the duties and responsibilities of the state agencies
1399 related to technology evaluation, purchasing, and cost savings.

1400 (7) DEPARTMENT OF LEGAL AFFAIRS, DEPARTMENT OF FINANCIAL
1401 SERVICES, AND DEPARTMENT OF AGRICULTURE AND CONSUMER SERVICES
1402 INFORMATION TECHNOLOGY STAFF.—Appropriate information technology
1403 staff of the Department of Legal Affairs, the Department of
1404 Financial Services, and the Department of Agriculture and
1405 Consumer Services shall participate in the workgroups created
1406 under subsections (1), (2), and (3) and may participate in any
1407 other workgroups as authorized by their respective elected
1408 official.

1409 Section 14. Section 282.0063, Florida Statutes, is created
1410 to read:

1411 282.0063 State information technology professionals career
1412 paths and training.—

1413 (1) DIGIT shall develop standardized frameworks for, and
1414 career paths, progressions, and training programs for, the
1415 benefit of state agency information technology personnel. To
1416 meet that goal, DIGIT shall:

1417 (a) Assess current and future information technology
1418 workforce needs across state agencies, identify skill gaps, and
1419 develop strategies to address them.

1420 (b) Develop and establish a training program for state
1421 agencies to support the understanding and implementation of each

31-01058B-26

2026480

1422 element of the enterprise architecture.

1423 (c) Establish training programs, certifications, and
1424 continuing education opportunities to enhance information
1425 technology competencies, including cybersecurity, cloud
1426 computing, and emerging technologies.

1427 (d) Support initiatives to provide existing employees with
1428 training or other opportunities to develop skills in emerging
1429 technologies and automation, ensuring that state agencies remain
1430 competitive and innovative.

1431 (e) Develop strategies to recruit and retain information
1432 technology professionals, including internship programs,
1433 apprenticeships, partnerships with educational institutions,
1434 scholarships for service, and initiatives to attract diverse
1435 talent.

1436 (2) DIGIT shall consult with CareerSource Florida, Inc.,
1437 the Department of Commerce, and the Department of Education in
1438 the implementation of this section.

1439 Section 15. Section 282.0064, Florida Statutes, is created
1440 to read:

1441 282.0064 Information technology contract policy.—

1442 (1) In coordination with the Department of Management
1443 Services, DIGIT shall establish a policy for all information
1444 technology-related solicitations and contracts, including state
1445 term contracts; contracts sourced using alternative purchasing
1446 methods as authorized pursuant to s. 287.042(16); sole source
1447 and emergency procurements; and contracts for commodities,
1448 consultant services, and staff augmentation services.

1449 (2) Related to state term contracts, the information
1450 technology policy must include:

31-01058B-26

2026480

1451 (a) Identification of the information technology product
1452 and service categories to be included in state term contracts.

1453 (b) The term of each information technology-related state
1454 term contract.

1455 (c) The maximum number of vendors authorized on each state
1456 term contract.

1457 (3) For all contracts, the information technology policy
1458 must include:

1459 (a) Evaluation criteria for the award of information
1460 technology-related contracts.

1461 (b) Requirements to be included in solicitations.

1462 (c) At a minimum, a requirement that any contract for
1463 information technology commodities or services meet the
1464 requirements of the enterprise architecture and National
1465 Institute of Standards and Technology Cybersecurity Framework.

1466 (4) The policy must include the following requirements for
1467 any information technology project that requires project
1468 oversight through independent verification and validation:

1469 (a) An entity providing independent verification and
1470 validation may not have any:

1471 1. Technical, managerial, or financial interest in the
1472 project; or

1473 2. Responsibility for or participation in any other aspect
1474 of the project.

1475 (b) The primary objective of independent verification and
1476 validation must be to provide an objective assessment throughout
1477 the entire project life cycle, reporting directly to all
1478 relevant stakeholders. An independent verification and
1479 validation entity shall independently verify and validate

31-01058B-26

2026480

1480 whether:

1481 1. The project is being built and implemented in accordance
1482 with defined technical architecture, specifications, and
1483 requirements.

1484 2. The project is adhering to established project
1485 management processes.

1486 3. The procurement of products, tools, and services and
1487 resulting contracts aligns with current statutory and regulatory
1488 requirements.

1489 4. The value of services delivered is commensurate with
1490 project costs.

1491 5. The completed project meets the actual needs of the
1492 intended users.

1493 (c) The entity performing independent verification and
1494 validation shall provide regular reports and assessments
1495 directly to the designated oversight body, identifying risks,
1496 deficiencies, and recommendations for corrective actions to
1497 ensure project success and compliance with statutory
1498 requirements.

1499 (5) The Division of State Purchasing in the Department of
1500 Management Services shall coordinate with DIGIT on state term
1501 contract solicitations and invitations to negotiate related to
1502 information technology. Such coordination must include DIGIT
1503 providing the Division of State Purchasing with an evaluation of
1504 vendor responses and assistance with answers to vendor questions
1505 on such solicitations or invitations to negotiate.

1506 (6) The Department of Legal Affairs, the Department of
1507 Financial Services, and the Department of Agriculture and
1508 Consumer Services may adopt alternatives to the information

31-01058B-26

2026480

1509 technology policy established by DIGIT pursuant to this section.
1510 If alternatives to the policy are adopted, such department must
1511 notify DIGIT, the Governor, the President of the Senate, and the
1512 Speaker of the House of Representatives in writing of the
1513 adoption of the alternatives and provide a justification for
1514 adoption of the alternatives, including whether the alternatives
1515 were necessary to meet alternatives adopted pursuant to s.
1516 282.00515, and explain the manner in which the department will
1517 achieve the information technology policy.

1518 Section 16. Subsections (3), (4), (7), and (10) of section
1519 282.318, Florida Statutes, are amended to read:

1520 282.318 Cybersecurity.—

1521 (3) DIGIT The department, acting through the Florida
1522 Digital Service, is the lead entity responsible for establishing
1523 standards and processes for assessing state agency cybersecurity
1524 risks and determining appropriate security measures that comply
1525 with all national and state data compliance security standards.
1526 Such standards and processes must be consistent with generally
1527 accepted technology best practices, including the National
1528 Institute for Standards and Technology Cybersecurity Framework,
1529 for cybersecurity. DIGIT The department, acting through the
1530 Florida Digital Service, shall adopt rules that mitigate risks;
1531 safeguard state agency digital assets, data, information, and
1532 information technology resources to ensure availability,
1533 confidentiality, and integrity; and support a security
1534 governance framework. DIGIT The department, acting through the
1535 Florida Digital Service, shall also:

1536 (a) Designate an employee of the Florida Digital Service as
1537 the state chief information security officer. The state chief

31-01058B-26

2026480

1538 information security officer must have experience and expertise
1539 in security and risk management for communications and
1540 information technology resources. The state chief information
1541 security officer is responsible for the development of
1542 enterprise cybersecurity policy, standards, operation, and
1543 security architecture oversight ~~of cybersecurity~~ for state
1544 technology systems. The state chief information security officer
1545 must ~~shall~~ be notified of all confirmed or suspected incidents
1546 or threats of state agency information technology resources and
1547 must report such incidents or threats to the state chief
1548 information officer ~~and the Governor~~.

1549 (b) Develop, and annually update by February 1, a statewide
1550 cybersecurity strategic plan that includes security goals and
1551 objectives for cybersecurity, including the identification and
1552 mitigation of risk, proactive protections against threats,
1553 tactical risk detection, threat reporting, and response and
1554 recovery protocols for a cyber incident.

1555 (c) Develop and publish for use by state agencies a
1556 cybersecurity governance framework that, at a minimum, includes
1557 guidelines and processes for:

1558 1. Establishing asset management procedures to ensure that
1559 an agency's information technology resources are identified and
1560 managed consistent with their relative importance to the
1561 agency's business objectives.

1562 2. Using a standard risk assessment methodology that
1563 includes the identification of an agency's priorities,
1564 constraints, risk tolerances, and assumptions necessary to
1565 support operational risk decisions.

1566 3. Completing comprehensive risk assessments and

31-01058B-26

2026480

1567 cybersecurity audits, which may be completed by a private sector
1568 vendor, and submitting completed assessments and audits to the
1569 department.

1570 4. Identifying protection procedures to manage the
1571 protection of an agency's information, data, and information
1572 technology resources.

1573 5. Establishing procedures for accessing information and
1574 data to ensure the confidentiality, integrity, and availability
1575 of such information and data.

1576 6. Detecting threats through proactive monitoring of
1577 events, continuous security monitoring, and defined detection
1578 processes.

1579 7. Establishing agency cybersecurity incident response
1580 teams and describing their responsibilities for responding to
1581 cybersecurity incidents, including breaches of personal
1582 information containing confidential or exempt data.

1583 8. Recovering information and data in response to a
1584 cybersecurity incident. The recovery may include recommended
1585 improvements to the agency processes, policies, or guidelines.

1586 9. Establishing a cybersecurity incident reporting process
1587 that includes procedures for notifying DIGIT the department and
1588 the Department of Law Enforcement of cybersecurity incidents.

1589 a. The level of severity of the cybersecurity incident is
1590 defined by the National Cyber Incident Response Plan of the
1591 United States Department of Homeland Security as follows:

1592 (I) Level 5 is an emergency-level incident within the
1593 specified jurisdiction that poses an imminent threat to the
1594 provision of wide-scale critical infrastructure services;
1595 national, state, or local government security; or the lives of

31-01058B-26

2026480

1596 the country's, state's, or local government's residents.

1597 (II) Level 4 is a severe-level incident that is likely to
1598 result in a significant impact in the affected jurisdiction to
1599 public health or safety; national, state, or local security;
1600 economic security; or civil liberties.

1601 (III) Level 3 is a high-level incident that is likely to
1602 result in a demonstrable impact in the affected jurisdiction to
1603 public health or safety; national, state, or local security;
1604 economic security; civil liberties; or public confidence.

1605 (IV) Level 2 is a medium-level incident that may impact
1606 public health or safety; national, state, or local security;
1607 economic security; civil liberties; or public confidence.

1608 (V) Level 1 is a low-level incident that is unlikely to
1609 impact public health or safety; national, state, or local
1610 security; economic security; civil liberties; or public
1611 confidence.

1612 b. The cybersecurity incident reporting process must
1613 specify the information that must be reported by a state agency
1614 following a cybersecurity incident or ransomware incident,
1615 which, at a minimum, must include the following:

1616 (I) A summary of the facts surrounding the cybersecurity
1617 incident or ransomware incident.

1618 (II) The date on which the state agency most recently
1619 backed up its data; the physical location of the backup, if the
1620 backup was affected; and if the backup was created using cloud
1621 computing.

1622 (III) The types of data compromised by the cybersecurity
1623 incident or ransomware incident.

1624 (IV) The estimated fiscal impact of the cybersecurity

31-01058B-26

2026480

1625 incident or ransomware incident.

1626 (V) In the case of a ransomware incident, the details of
1627 the ransom demanded.

1628 c.(I) A state agency shall report all ransomware incidents
1629 and any cybersecurity incident determined by the state agency to
1630 be of severity level 3, 4, or 5 to the state chief information
1631 security officer Cybersecurity Operations Center and the
1632 Cybercrime Office of the Department of Law Enforcement as soon
1633 as possible but no later than 48 hours after discovery of the
1634 cybersecurity incident and no later than 12 hours after
1635 discovery of the ransomware incident. The report must contain
1636 the information required in sub-subparagraph b. If the event
1637 involves services housed or procured through the Northwest
1638 Regional Data Center, the state agency must also notify the
1639 Northwest Regional Data Center.

1640 (II) The state chief information security officer
1641 Cybersecurity Operations Center shall notify the President of
1642 the Senate and the Speaker of the House of Representatives of
1643 any severity level 3, 4, or 5 incident as soon as possible but
1644 no later than 12 hours after receiving a state agency's incident
1645 report. The notification must include a high-level description
1646 of the incident and the likely effects.

1647 d. A state agency shall report a cybersecurity incident
1648 determined by the state agency to be of severity level 1 or 2 to
1649 the state chief information security officer Cybersecurity
1650 Operations Center and the Cybercrime Office of the Department of
1651 Law Enforcement as soon as possible, but no later than 96 hours
1652 after the discovery of the cybersecurity incident and no later
1653 than 72 hours after the discovery of the ransomware incident.

31-01058B-26

2026480

1654 The report must contain the information required in sub-
1655 subparagraph b. If the event involves services housed or
1656 procured through the Northwest Regional Data Center, the state
1657 agency must also notify the Northwest Regional Data Center.

1658 e. The state chief information security officer
1659 ~~Cybersecurity Operations Center~~ shall provide a consolidated
1660 incident report on a quarterly basis to the President of the
1661 Senate ~~and,~~ the Speaker of the House of Representatives, ~~and the~~
1662 ~~Florida Cybersecurity Advisory Council~~. The ~~report provided to~~
1663 ~~the Florida Cybersecurity Advisory Council may not contain the~~
1664 ~~name of any agency, network information, or system identifying~~
1665 ~~information but must contain sufficient relevant information to~~
1666 ~~allow the Florida Cybersecurity Advisory Council to fulfill its~~
1667 ~~responsibilities as required in s. 282.319(9).~~

1668 10. Incorporating information obtained through detection
1669 and response activities into the agency's cybersecurity incident
1670 response plans.

1671 11. Developing agency strategic and operational
1672 cybersecurity plans required pursuant to this section.

1673 12. Establishing the managerial, operational, and technical
1674 safeguards for protecting state government data and information
1675 technology resources that align with the state agency risk
1676 management strategy and that protect the confidentiality,
1677 integrity, and availability of information and data.

1678 13. Establishing procedures for procuring information
1679 technology commodities and services that require the commodity
1680 or service to meet the National Institute of Standards and
1681 Technology Cybersecurity Framework.

1682 14. Submitting after-action reports following a

31-01058B-26

2026480

1683 cybersecurity incident or ransomware incident. Such guidelines
1684 and processes for submitting after-action reports must be
1685 developed and published by December 1, 2022.

1686 (d) Assist state agencies in complying with this section.

1687 (e) In collaboration with the Cybercrime Office of the
1688 Department of Law Enforcement, annually provide training for
1689 state agency information security managers and computer security
1690 incident response team members that contains training on
1691 cybersecurity, including cybersecurity threats, trends, and best
1692 practices.

1693 (f) Annually review the strategic and operational
1694 cybersecurity plans of state agencies.

1695 (g) Annually provide cybersecurity training to all state
1696 agency technology professionals and employees with access to
1697 highly sensitive information which develops, assesses, and
1698 documents competencies by role and skill level. The
1699 cybersecurity training curriculum must include training on the
1700 identification of each cybersecurity incident severity level
1701 referenced in sub subparagraph (c)9.a. The training may be
1702 provided in collaboration with the Cybercrime Office of the
1703 Department of Law Enforcement, a private sector entity, or an
1704 institution of the State University System.

1705 (h) ~~Operate and maintain a Cybersecurity Operations Center~~
1706 ~~led by the state chief information security officer, which must~~
1707 ~~be primarily virtual and staffed with tactical detection and~~
1708 ~~incident response personnel. The Cybersecurity Operations Center~~
1709 ~~shall serve as a clearinghouse for threat information and~~
1710 ~~coordinate with the Department of Law Enforcement to support~~
1711 ~~state agencies and their response to any confirmed or suspected~~

31-01058B-26

2026480

1712 cybersecurity incident.

1713 (i) Lead an Emergency Support Function, ESF CYBER, under
1714 the state comprehensive emergency management plan as described
1715 in s. 252.35.

1716 (4) Each state agency head shall, at a minimum:

1717 (a) Designate an information security manager to administer
1718 the cybersecurity program of the state agency. This designation
1719 must be provided annually in writing to DIGIT the department by
1720 January 1. A state agency's information security manager, for
1721 purposes of these information security duties, shall report
1722 directly to the agency head.

1723 (b) In consultation with the state chief information
1724 security officer department, through the Florida Digital
1725 Service, and the Cybercrime Office of the Department of Law
1726 Enforcement, establish an agency cybersecurity response team to
1727 respond to a cybersecurity incident. The agency cybersecurity
1728 response team shall convene upon notification of a cybersecurity
1729 incident and shall ~~must~~ immediately report all confirmed or
1730 suspected incidents to the state chief information security
1731 officer, or his or her designee, and comply with all applicable
1732 guidelines and processes established pursuant to paragraph
1733 (3) (c).

1734 (c) Submit to the state chief information security officer
1735 ~~department~~ annually by July 31, the state agency's strategic and
1736 operational cybersecurity plans developed pursuant to rules and
1737 guidelines established by the state chief information security
1738 officer department, through the Florida Digital Service.

1739 1. The state agency strategic cybersecurity plan must cover
1740 a 2-year ~~3-year~~ period and, at a minimum, define security goals,

31-01058B-26

2026480

1741 intermediate objectives, and projected agency costs for the
1742 strategic issues of agency information security policy, risk
1743 management, security training, security incident response, and
1744 disaster recovery. The plan must be based on the statewide
1745 cybersecurity strategic plan created by the state chief
1746 information security officer department and include performance
1747 metrics that can be objectively measured to reflect the status
1748 of the state agency's progress in meeting security goals and
1749 objectives identified in the agency's strategic information
1750 security plan.

1751 2. The state agency operational cybersecurity plan must
1752 include a set of measures that objectively assess the
1753 performance of the agency's cybersecurity program in accordance
1754 with its risk management plan progress report that objectively
1755 measures progress made towards the prior operational
1756 cybersecurity plan and a project plan that includes activities,
1757 timelines, and deliverables for security objectives that the
1758 state agency will implement during the current fiscal year.

1759 (d) Conduct, and update every 2 3 years, a comprehensive
1760 risk assessment, which may be completed by a private sector
1761 vendor, to determine the security threats to the data,
1762 information, and information technology resources, including
1763 mobile devices and print environments, of the agency. The risk
1764 assessment must comply with the risk assessment methodology
1765 developed by the state chief information security officer
1766 department and is confidential and exempt from s. 119.07(1),
1767 except that such information shall be available to the Auditor
1768 General, the state chief information security officer Florida
1769 Digital Service within the department, the Cybercrime Office of

31-01058B-26

2026480

1770 the Department of Law Enforcement, and, for state agencies under
1771 the jurisdiction of the Governor, the Chief Inspector General.
1772 If a private sector vendor is used to complete a comprehensive
1773 risk assessment, it must attest to the validity of the risk
1774 assessment findings. The comprehensive risk assessment must
1775 include all of the following:

1776 1. The results of vulnerability and penetration tests on
1777 any Internet website or mobile application that processes any
1778 sensitive personal information or confidential information and a
1779 plan to address any vulnerability identified in the tests.

1780 2. A written acknowledgment that the executive director or
1781 the secretary of the agency, the chief financial officer of the
1782 agency, and each executive manager as designated by the state
1783 agency have been made aware of the risks revealed during the
1784 preparation of the agency's operations cybersecurity plan and
1785 the comprehensive risk assessment.

1786 (e) Develop, and periodically update, written internal
1787 policies and procedures, which include procedures for reporting
1788 cybersecurity incidents and breaches to the Cybercrime Office of
1789 the Department of Law Enforcement and the state chief
1790 information security officer Florida Digital Service within the
1791 department. Such policies and procedures must be consistent with
1792 the rules, guidelines, and processes established by DIGIT the
1793 department to ensure the security of the data, information, and
1794 information technology resources of the agency. The internal
1795 policies and procedures that, if disclosed, could facilitate the
1796 unauthorized modification, disclosure, or destruction of data or
1797 information technology resources are confidential information
1798 and exempt from s. 119.07(1), except that such information must

31-01058B-26

2026480

1799 shall be available to the Auditor General, the Cybercrime Office
1800 of the Department of Law Enforcement, the state chief
1801 information security officer ~~the Florida Digital Service within~~
1802 ~~the department~~, and, for state agencies under the jurisdiction
1803 of the Governor, the Chief Inspector General.

1804 (f) Implement managerial, operational, and technical
1805 safeguards and risk assessment remediation plans recommended by
1806 DIGIT ~~the department~~ to address identified risks to the data,
1807 information, and information technology resources of the agency.
1808 The state chief information security officer ~~department, through~~
1809 ~~the Florida Digital Service,~~ shall track implementation by state
1810 agencies upon development of such remediation plans in
1811 coordination with agency inspectors general.

1812 (g) Ensure that periodic internal audits and evaluations of
1813 the agency's cybersecurity program for the data, information,
1814 and information technology resources of the agency are
1815 conducted. The results of such audits and evaluations are
1816 confidential information and exempt from s. 119.07(1), except
1817 that such information must ~~shall~~ be available to the Auditor
1818 General, the Cybercrime Office of the Department of Law
1819 Enforcement, the state chief information security officer
1820 ~~Florida Digital Service within the department~~, and, for agencies
1821 under the jurisdiction of the Governor, the Chief Inspector
1822 General.

1823 (h) Ensure that the cybersecurity requirements in the
1824 written specifications for the solicitation, contracts, and
1825 service-level agreement of information technology and
1826 information technology resources and services meet or exceed the
1827 applicable state and federal laws, regulations, and standards

31-01058B-26

2026480

1828 for cybersecurity, including the National Institute of Standards
1829 and Technology Cybersecurity Framework. Service-level agreements
1830 must identify service provider and state agency responsibilities
1831 for privacy and security, protection of government data,
1832 personnel background screening, and security deliverables with
1833 associated frequencies.

1834 (i) Provide cybersecurity awareness training to all state
1835 agency employees within 30 days after commencing employment, and
1836 annually thereafter, concerning cybersecurity risks and the
1837 responsibility of employees to comply with policies, standards,
1838 guidelines, and operating procedures adopted by the state agency
1839 to reduce those risks. The training may be provided in
1840 collaboration with the Cybercrime Office of the Department of
1841 Law Enforcement, a private sector entity, or an institution of
1842 the State University System.

1843 (j) Develop a process for detecting, reporting, and
1844 responding to threats, breaches, or cybersecurity incidents
1845 which is consistent with the security rules, guidelines, and
1846 processes established by DIGIT the department through the state
1847 chief information security officer ~~Florida Digital Service~~.

1848 1. All cybersecurity incidents and ransomware incidents
1849 must be reported by state agencies. Such reports must comply
1850 with the notification procedures and reporting timeframes
1851 established pursuant to paragraph (3) (c).

1852 2. For cybersecurity breaches, state agencies shall provide
1853 notice in accordance with s. 501.171.

1854 (k) Submit to the state chief information security officer
1855 ~~Florida Digital Service~~, within 1 week after the remediation of
1856 a cybersecurity incident or ransomware incident, an after-action

31-01058B-26

2026480

1857 report that summarizes the incident, the incident's resolution,
1858 and any insights gained as a result of the incident.

1859 (7) The portions of records made confidential and exempt in
1860 subsections (5) and (6) must ~~shall~~ be available to the Auditor
1861 General, the Cybercrime Office of the Department of Law
1862 Enforcement, the state chief information security officer, the
1863 Legislature ~~Florida Digital Service within the department~~, and,
1864 for agencies under the jurisdiction of the Governor, the Chief
1865 Inspector General. Such portions of records may be made
1866 available to a local government, another state agency, or a
1867 federal agency for cybersecurity purposes or in furtherance of
1868 the state agency's official duties.

1869 (10) DIGIT ~~The department~~ shall adopt rules relating to
1870 cybersecurity and to administer this section.

1871 Section 17. Subsections (3) through (6) of section
1872 282.3185, Florida Statutes, are amended to read:

1873 282.3185 Local government cybersecurity.—

1874 (3) CYBERSECURITY TRAINING.—

1875 (a) The state chief information security officer ~~Florida~~
1876 ~~Digital Service~~ shall:

1877 1. Develop a basic cybersecurity training curriculum for
1878 local government employees. All local government employees with
1879 access to the local government's network must complete the basic
1880 cybersecurity training within 30 days after commencing
1881 employment and annually thereafter.

1882 2. Develop an advanced cybersecurity training curriculum
1883 for local governments which is consistent with the cybersecurity
1884 training required under s. 282.318(3)(f) ~~s. 282.318(3)(g)~~. All
1885 local government technology professionals and employees with

31-01058B-26

2026480

1886 access to highly sensitive information must complete the
1887 advanced cybersecurity training within 30 days after commencing
1888 employment and annually thereafter.

1889 (b) The state chief information security officer Florida
1890 ~~Digital Service~~ may provide the cybersecurity training required
1891 by this subsection in collaboration with the Cybercrime Office
1892 of the Department of Law Enforcement, a private sector entity,
1893 or an institution of the State University System.

1894 (4) CYBERSECURITY STANDARDS.—

1895 (a) Each local government shall adopt cybersecurity
1896 standards that safeguard its data, information technology, and
1897 information technology resources to ensure availability,
1898 confidentiality, and integrity. The cybersecurity standards must
1899 be consistent with generally accepted best practices for
1900 cybersecurity, including the National Institute of Standards and
1901 Technology Cybersecurity Framework.

1902 (b) ~~Each county with a population of 75,000 or more must~~
1903 ~~adopt the cybersecurity standards required by this subsection by~~
1904 ~~January 1, 2024. Each county with a population of less than~~
1905 ~~75,000 must adopt the cybersecurity standards required by this~~
1906 ~~subsection by January 1, 2025.~~

1907 (c) ~~Each municipality with a population of 25,000 or more~~
1908 ~~must adopt the cybersecurity standards required by this~~
1909 ~~subsection by January 1, 2024. Each municipality with a~~
1910 ~~population of less than 25,000 must adopt the cybersecurity~~
1911 ~~standards required by this subsection by January 1, 2025.~~

1912 (d) Each local government shall notify the state chief
1913 information security officer Florida ~~Digital Service~~ of its
1914 compliance with this subsection as soon as possible.

31-01058B-26

2026480

1915 (5) INCIDENT NOTIFICATION.—

1916 (a) A local government shall provide notification of a
1917 cybersecurity incident or ransomware incident to the state chief
1918 information security officer ~~Cybersecurity Operations Center~~,
1919 the Cybercrime Office of the Department of Law Enforcement, and
1920 the sheriff who has jurisdiction over the local government in
1921 accordance with paragraph (b). The notification must include, at
1922 a minimum, the following information:

1923 1. A summary of the facts surrounding the cybersecurity
1924 incident or ransomware incident.

1925 2. The date on which the local government most recently
1926 backed up its data; the physical location of the backup, if the
1927 backup was affected; and if the backup was created using cloud
1928 computing.

1929 3. The types of data compromised by the cybersecurity
1930 incident or ransomware incident.

1931 4. The estimated fiscal impact of the cybersecurity
1932 incident or ransomware incident.

1933 5. In the case of a ransomware incident, the details of the
1934 ransom demanded.

1935 6. A statement requesting or declining assistance from ~~the~~
1936 ~~Cybersecurity Operations Center~~, the Cybercrime Office of the
1937 Department of Law Enforcement, or the sheriff who has
1938 jurisdiction over the local government.

1939 (b) 1. A local government shall report all ransomware
1940 incidents and any cybersecurity incident determined by the local
1941 government to be of severity level 3, 4, or 5 as provided in s.
1942 282.318(3)(b) ~~s. 282.318(3)(e)~~ to the state chief information
1943 security officer ~~Cybersecurity Operations Center~~, the Cybercrime

31-01058B-26

2026480

1944 Office of the Department of Law Enforcement, and the sheriff who
1945 has jurisdiction over the local government as soon as possible
1946 but no later than 12 48 hours after discovery of the
1947 cybersecurity incident and no later than 6 12 hours after
1948 discovery of the ransomware incident. The report must contain
1949 the information required in paragraph (a).

1950 2. The state chief information security officer

1951 ~~Cybersecurity Operations Center~~ shall notify the President of
1952 the Senate and the Speaker of the House of Representatives of
1953 any severity level 3, 4, or 5 incident as soon as possible but
1954 no later than 12 hours after receiving a local government's
1955 incident report. The notification must include a high-level
1956 description of the incident and the likely effects.

1957 (c) A local government may report a cybersecurity incident
1958 determined by the local government to be of severity level 1 or
1959 2 as provided in s. 282.318(3)(b) ~~s. 282.318(3)(c)~~ to the state
1960 chief information security officer ~~Cybersecurity Operations~~
1961 ~~Center~~, the Cybercrime Office of the Department of Law
1962 Enforcement, and the sheriff who has jurisdiction over the local
1963 government. The report must ~~shall~~ contain the information
1964 required in paragraph (a).

1965 (d) The state chief information security officer

1966 ~~Cybersecurity Operations Center~~ shall provide a consolidated
1967 incident report by the 30th day after the end of each quarter ~~on~~
1968 ~~a quarterly basis~~ to the President of the Senate, and the
1969 Speaker of the House of Representatives, ~~and the Florida~~
1970 ~~Cybersecurity Advisory Council~~. The report ~~provided to the~~
1971 ~~Florida Cybersecurity Advisory Council~~ may not contain the name
1972 ~~of any local government, network information, or system~~

31-01058B-26

2026480

1973 identifying information but must contain sufficient relevant
1974 information to allow the Florida Cybersecurity Advisory Council
1975 to fulfill its responsibilities as required in s. 282.319(9).

1976 (6) AFTER-ACTION REPORT.—A local government shall ~~must~~
1977 submit to the state chief information security officer ~~Florida~~
1978 ~~Digital Service~~, within 1 week after the remediation of a
1979 cybersecurity incident or ransomware incident, an after-action
1980 report that summarizes the incident, the incident's resolution,
1981 and any insights gained as a result of the incident. ~~By December~~
1982 ~~1, 2022, the Florida Digital Service shall establish guidelines~~
1983 ~~and processes for submitting an after-action report.~~

1984 Section 18. Section 282.319, Florida Statutes, is repealed.

1985 Section 19. Section 282.201, Florida Statutes, is amended
1986 to read:

1987 282.201 State data center.—The state data center is
1988 established within the Northwest Regional Data Center pursuant
1989 to s. 282.2011 and shall meet or exceed the information
1990 technology standards specified in ss. 282.006 and 282.318 ~~the~~
1991 ~~department. The provision of data center services must comply~~
1992 ~~with applicable state and federal laws, regulations, and~~
1993 ~~policies, including all applicable security, privacy, and~~
1994 ~~auditing requirements. The department shall appoint a director~~
1995 ~~of the state data center who has experience in leading data~~
1996 ~~center facilities and has expertise in cloud computing~~
1997 ~~management.~~

1998 (1) STATE DATA CENTER DUTIES. The state data center shall:

1999 (a) ~~Offer, develop, and support the services and~~
2000 ~~applications defined in service-level agreements executed with~~
2001 ~~its customer entities.~~

31-01058B-26

2026480

2002 (b) ~~Maintain performance of the state data center by ensuring proper data backup; data backup recovery; disaster recovery; and appropriate security, power, cooling, fire suppression, and capacity.~~

2003 (c) ~~Develop and implement business continuity and disaster recovery plans, and annually conduct a live exercise of each plan.~~

2004 (d) ~~Enter into a service level agreement with each customer entity to provide the required type and level of service or services. If a customer entity fails to execute an agreement within 60 days after commencement of a service, the state data center may cease service. A service level agreement may not have a term exceeding 3 years and at a minimum must:~~

2005 1. ~~Identify the parties and their roles, duties, and responsibilities under the agreement.~~

2006 2. ~~State the duration of the contract term and specify the conditions for renewal.~~

2007 3. ~~Identify the scope of work.~~

2008 4. ~~Identify the products or services to be delivered with sufficient specificity to permit an external financial or performance audit.~~

2009 5. ~~Establish the services to be provided, the business standards that must be met for each service, the cost of each service by agency application, and the metrics and processes by which the business standards for each service are to be objectively measured and reported.~~

2010 6. ~~Provide a timely billing methodology to recover the costs of services provided to the customer entity pursuant to s.~~

2011 215.422.

31-01058B-26

2026480

2031 7. Provide a procedure for modifying the service level
2032 agreement based on changes in the type, level, and cost of a
2033 service.

2034 8. Include a right-to-audit clause to ensure that the
2035 parties to the agreement have access to records for audit
2036 purposes during the term of the service level agreement.

2037 9. Provide that a service level agreement may be terminated
2038 by either party for cause only after giving the other party and
2039 the department notice in writing of the cause for termination
2040 and an opportunity for the other party to resolve the identified
2041 cause within a reasonable period.

2042 10. Provide for mediation of disputes by the Division of
2043 Administrative Hearings pursuant to s. 120.573.

2044 (e) For purposes of chapter 273, be the custodian of
2045 resources and equipment located in and operated, supported, and
2046 managed by the state data center.

2047 (f) Assume administrative access rights to resources and
2048 equipment, including servers, network components, and other
2049 devices, consolidated into the state data center.

2050 1. Upon consolidation, a state agency shall relinquish
2051 administrative rights to consolidated resources and equipment.
2052 State agencies required to comply with federal and state
2053 criminal justice information security rules and policies shall
2054 retain administrative access rights sufficient to comply with
2055 the management control provisions of those rules and policies;
2056 however, the state data center shall have the appropriate type
2057 or level of rights to allow the center to comply with its duties
2058 pursuant to this section. The Department of Law Enforcement
2059 shall serve as the arbiter of disputes pertaining to the

31-01058B-26

2026480

2060 appropriate type and level of administrative access rights
2061 pertaining to the provision of management control in accordance
2062 with the federal criminal justice information guidelines.

2063 2. The state data center shall provide customer entities
2064 with access to applications, servers, network components, and
2065 other devices necessary for entities to perform business
2066 activities and functions, and as defined and documented in a
2067 service level agreement.

2068 (g) In its procurement process, show preference for cloud-
2069 computing solutions that minimize or do not require the
2070 purchasing, financing, or leasing of state data center
2071 infrastructure, and that meet the needs of customer agencies,
2072 that reduce costs, and that meet or exceed the applicable state
2073 and federal laws, regulations, and standards for cybersecurity.

2074 (h) Assist customer entities in transitioning from state
2075 data center services to the Northwest Regional Data Center or
2076 other third-party cloud computing services procured by a
2077 customer entity or by the Northwest Regional Data Center on
2078 behalf of a customer entity.

2079 (1) ~~(2)~~ USE OF THE STATE DATA CENTER.—

2080 (a) The following are exempt from the use of the state data
2081 center: the Department of Law Enforcement, the Department of the
2082 Lottery's Gaming System, Systems Design and Development in the
2083 Office of Policy and Budget, the regional traffic management
2084 centers as described in s. 335.14(2) and the Office of Toll
2085 Operations of the Department of Transportation, the State Board
2086 of Administration, state attorneys, public defenders, criminal
2087 conflict and civil regional counsel, capital collateral regional
2088 counsel, and the Florida Housing Finance Corporation, and the

31-01058B-26

2026480

2089 Division of Emergency Management within the Executive Office of
2090 the Governor.

2091 ~~(b) The Division of Emergency Management is exempt from the~~
2092 ~~use of the state data center. This paragraph expires July 1,~~
2093 ~~2026.~~

2094 ~~(2) (3) AGENCY LIMITATIONS.~~—Unless exempt from the use of
2095 the state data center pursuant to this section or authorized by
2096 the Legislature, a state agency may not:

2097 (a) Create a new agency computing facility or data center,
2098 or expand the capability to support additional computer
2099 equipment in an existing agency computing facility or data
2100 center; or

2101 (b) Terminate services with the state data center without
2102 giving written notice of intent to terminate services 180 days
2103 before such termination.

2104 ~~(4) DEPARTMENT RESPONSIBILITIES.~~—~~The department shall~~
2105 ~~provide operational management and oversight of the state data~~
2106 ~~center, which includes:~~

2107 ~~(a) Implementing industry standards and best practices for~~
2108 ~~the state data center's facilities, operations, maintenance,~~
2109 ~~planning, and management processes.~~

2110 ~~(b) Developing and implementing cost-recovery mechanisms~~
2111 ~~that recover the full direct and indirect cost of services~~
2112 ~~through charges to applicable customer entities. Such cost-~~
2113 ~~recovery mechanisms must comply with applicable state and~~
2114 ~~federal regulations concerning distribution and use of funds and~~
2115 ~~must ensure that, for any fiscal year, no service or customer~~
2116 ~~entity subsidizes another service or customer entity. The~~
2117 ~~department may recommend other payment mechanisms to the~~

31-01058B-26

2026480

2118 Executive Office of the Governor, the President of the Senate,
2119 and the Speaker of the House of Representatives. Such mechanisms
2120 may be implemented only if specifically authorized by the
2121 Legislature.

2122 (e) Developing and implementing appropriate operating
2123 guidelines and procedures necessary for the state data center to
2124 perform its duties pursuant to subsection (1). The guidelines
2125 and procedures must comply with applicable state and federal
2126 laws, regulations, and policies and conform to generally
2127 accepted governmental accounting and auditing standards. The
2128 guidelines and procedures must include, but need not be limited
2129 to:

2130 1. Implementing a consolidated administrative support
2131 structure responsible for providing financial management,
2132 procurement, transactions involving real or personal property,
2133 human resources, and operational support.

2134 2. Implementing an annual reconciliation process to ensure
2135 that each customer entity is paying for the full direct and
2136 indirect cost of each service as determined by the customer
2137 entity's use of each service.

2138 3. Providing rebates that may be credited against future
2139 billings to customer entities when revenues exceed costs.

2140 4. Requiring customer entities to validate that sufficient
2141 funds exist before implementation of a customer entity's request
2142 for a change in the type or level of service provided, if such
2143 change results in a net increase to the customer entity's cost
2144 for that fiscal year.

2145 5. By November 15 of each year, providing to the Office of
2146 Policy and Budget in the Executive Office of the Governor and to

31-01058B-26

2026480

2147 the chairs of the legislative appropriations committees the
2148 projected costs of providing data center services for the
2149 following fiscal year.

2150 6. Providing a plan for consideration by the Legislative
2151 Budget Commission if the cost of a service is increased for a
2152 reason other than a customer entity's request made pursuant to
2153 subparagraph 4. Such a plan is required only if the service cost
2154 increase results in a net increase to a customer entity for that
2155 fiscal year.

2156 7. Standardizing and consolidating procurement and
2157 contracting practices.

2158 (d) In collaboration with the Department of Law Enforcement
2159 and the Florida Digital Service, developing and implementing a
2160 process for detecting, reporting, and responding to
2161 cybersecurity incidents, breaches, and threats.

2162 (e) Adopting rules relating to the operation of the state
2163 data center, including, but not limited to, budgeting and
2164 accounting procedures, cost-recovery methodologies, and
2165 operating procedures.

2166 (5) NORTHWEST REGIONAL DATA CENTER CONTRACT. In order for
2167 the department to carry out its duties and responsibilities
2168 relating to the state data center, the secretary of the
2169 department shall contract by July 1, 2022, with the Northwest
2170 Regional Data Center pursuant to s. 287.057(11). The contract
2171 shall provide that the Northwest Regional Data Center will
2172 manage the operations of the state data center and provide data
2173 center services to state agencies.

2174 (a) The department shall provide contract oversight,
2175 including, but not limited to, reviewing invoices provided by

31-01058B-26

2026480

2176 the Northwest Regional Data Center for services provided to
2177 state agency customers.

2178 (b) The department shall approve or request updates to
2179 invoices within 10 business days after receipt. If the
2180 department does not respond to the Northwest Regional Data
2181 Center, the invoice will be approved by default. The Northwest
2182 Regional Data Center must submit approved invoices directly to
2183 state agency customers.

2184 Section 20. Section 282.2011, Florida Statutes, is created
2185 to read:

2186 282.2011 Northwest Regional Data Center.—

2187 (1) For the purpose of providing data center services to
2188 its state agency customers, the Northwest Regional Data Center
2189 is designated as the state data center for all state agencies,
2190 except as otherwise provided by law, and shall:

2191 (a) Operate under a governance structure that represents
2192 its customers proportionally.

2193 (b) Maintain an appropriate cost-allocation methodology
2194 that accurately bills state agency customers based solely on the
2195 actual direct and indirect costs of the services provided to
2196 state agency customers and ensures that, for any fiscal year,
2197 state agency customers are not subsidizing other customers of
2198 the data center. Such cost-allocation methodology must comply
2199 with applicable state and federal regulations concerning the
2200 distribution and use of state and federal funds.

2201 (c) Enter into a service-level agreement with each state
2202 agency customer to provide services as defined and approved by
2203 the governing board of the center. At a minimum, such service-
2204 level agreements must:

31-01058B-26

2026480

2205 1. Identify the parties and their roles, duties, and
2206 responsibilities under the agreement;
2207 2. State the duration of the agreement term, which may not
2208 exceed 3 years, and specify the conditions for up to two
2209 optional 1-year renewals of the agreement before execution of a
2210 new agreement;
2211 3. Identify the scope of work;
2212 4. Establish the services to be provided, the business
2213 standards that must be met for each service, the cost of each
2214 service, and the process by which the business standards for
2215 each service are to be objectively measured and reported;
2216 5. Provide a timely billing methodology for recovering the
2217 cost of services provided pursuant to s. 215.422;
2218 6. Provide a procedure for modifying the service-level
2219 agreement to address any changes in projected costs of service;
2220 7. Include a right-to-audit clause to ensure that the
2221 parties to the agreement have access to records for audit
2222 purposes during the term of the service-level agreement;
2223 8. Identify the products or services to be delivered with
2224 sufficient specificity to permit an external financial or
2225 performance audit;
2226 9. Provide that the service-level agreement may be
2227 terminated by either party for cause only after giving the other
2228 party notice in writing of the cause for termination and an
2229 opportunity for the other party to resolve the identified cause
2230 within a reasonable period; and
2231 10. Provide state agency customer entities with access to
2232 applications, servers, network components, and other devices
2233 necessary for entities to perform business activities and

31-01058B-26

2026480

2234 functions and as defined and documented in a service-level
2235 agreement.

2236 (d) In its procurement process, show preference for cloud-
2237 computing solutions that minimize or do not require the
2238 purchasing or financing of state data center infrastructure,
2239 that meet the needs of state agency customer entities, that
2240 reduce costs, and that meet or exceed the applicable state and
2241 federal laws, regulations, and standards for cybersecurity.

2242 (e) Assist state agency customer entities in transitioning
2243 from state data center services to other third-party cloud-
2244 computing services procured by a customer entity or by the
2245 Northwest Regional Data Center on behalf of the customer entity.

2246 (f) Provide to the Board of Governors the total annual
2247 budget by major expenditure category, including, but not limited
2248 to, salaries, expenses, operating capital outlay, contracted
2249 services, or other personnel services, by July 30 each fiscal
2250 year.

2251 (g) Provide to each state agency customer its projected
2252 annual cost for providing the agreed-upon data center services
2253 by September 1 each fiscal year.

2254 (h) By November 15 of each year, provide to the Office of
2255 Policy and Budget in the Executive Office of the Governor and to
2256 the chairs of the legislative appropriations committees the
2257 projected costs of providing data center services for the
2258 following fiscal year.

2259 (i) Provide a plan for consideration by the Legislative
2260 Budget Commission if the governing body of the center approves
2261 the use of a billing rate schedule after the start of the fiscal
2262 year that increases any state agency customer's costs for that

31-01058B-26

2026480

2263 fiscal year.2264 (j) Provide data center services that comply with
2265 applicable state and federal laws, regulations, and policies,
2266 including all applicable security, privacy, and auditing
2267 requirements.2268 (k) Maintain performance of the data center facilities by
2269 ensuring proper data backup; data backup recovery; disaster
2270 recovery; and appropriate security, power, cooling, fire
2271 suppression, and capacity.2272 (l) Submit invoices to state agency customers.2273 (m) As funded in the General Appropriations Act, provide
2274 data center services to state agencies from multiple facilities.2275 (2) Unless exempt from the requirement to use the state
2276 data center pursuant to s. 282.201(1) or as authorized by the
2277 Legislature, a state agency may not do any of the following:2278 (a) Terminate services with the Northwest Regional Data
2279 Center without giving written notice of intent to terminate
2280 services 180 days before such termination.2281 (b) Procure third-party cloud-computing services without
2282 evaluating the cloud-computing services provided by the
2283 Northwest Regional Data Center.2284 (c) Exceed 30 days from receipt of approved invoices to
2285 remit payment for state data center services provided by the
2286 Northwest Regional Data Center.2287 (3) The Northwest Regional Data Center's authority to
2288 provide data center services to its state agency customers may
2289 be terminated if:2290 (a) The center requests such termination to the Board of
2291 Governors, the President of the Senate, and the Speaker of the

31-01058B-26

2026480

2292 House of Representatives; or

2293 (b) The center fails to comply with the provisions of this
2294 section.

2295 (4) The Northwest Regional Data Center is the lead entity
2296 responsible for creating, operating, and managing, including the
2297 research conducted by, the Florida Behavioral Health Care Data
2298 Repository as established by this subsection.

2299 (a) The purpose of the data repository is to create a
2300 centralized system for:

2301 1. Collecting and analyzing existing statewide behavioral
2302 health care data to:

2303 a. Better understand the scope of and trends in behavioral
2304 health services, spending, and outcomes to improve patient care
2305 and enhance the efficiency and effectiveness of behavioral
2306 health services;

2307 b. Better understand the scope of, trends in, and
2308 relationship between behavioral health, criminal justice,
2309 incarceration, and the use of behavioral health services as a
2310 diversion from incarceration for individuals with mental
2311 illness; and

2312 c. Enhance the collection and coordination of treatment and
2313 outcome information as an ongoing evidence base for research and
2314 education related to behavioral health.

2315 2. Developing useful data analytics, economic metrics, and
2316 visual representations of such analytics and metrics to inform
2317 relevant state agencies and the Legislature of data and trends
2318 in behavioral health.

2319 (b) The Northwest Regional Data Center shall develop, in
2320 collaboration with the Data Analysis Committee of the Commission

31-01058B-26

2026480

2321 on Mental Health and Substance Use Disorder created under s.
2322 394.9086 and with relevant stakeholders, a plan that includes
2323 all of the following:

2324 1. A project plan that describes the technology,
2325 methodology, timeline, cost, and resources necessary to create a
2326 centralized, integrated, and coordinated data system.

2327 2. A proposed governance structure to oversee the
2328 implementation and operations of the repository.

2329 3. An integration strategy to incorporate existing data
2330 from relevant state agencies, including, but not limited to, the
2331 Agency for Health Care Administration, the Department of
2332 Children and Families, the Department of Juvenile Justice, the
2333 Office of the State Courts Administrator, and the Department of
2334 Corrections.

2335 4. Identification of relevant data and metrics to support
2336 actionable information and ensure the efficient and responsible
2337 use of taxpayer dollars within behavioral health systems of
2338 care.

2339 5. Data security requirements for the repository.

2340 6. The structure and process that will be used to create an
2341 annual analysis and report that gives state agencies and the
2342 Legislature a better general understanding of trends and issues
2343 in the state's behavioral health systems of care and the trends
2344 and issues in behavioral health systems related to criminal
2345 justice treatment, diversion, and incarceration.

2346 (c) Beginning December 1, 2026, and annually thereafter,
2347 the Northwest Regional Data Center shall submit the developed
2348 trends and issues report under subparagraph (b) 6. to the
2349 Governor, the President of the Senate, and the Speaker of the

31-01058B-26

2026480

2350 House of Representatives.

2351 (5) If such authority is terminated, the center has 1 year
2352 to provide for the transition of its state agency customers to a
2353 qualified alternative cloud-based data center that meets the
2354 enterprise architecture standards established pursuant to this
2355 chapter.

2356 Section 21. Subsection (4) of section 282.206, Florida
2357 Statutes, is amended to read:

2358 282.206 Cloud-first policy in state agencies.—

2359 (4) Each state agency shall develop a strategic plan to be
2360 updated annually to address its inventory of applications
2361 located at the state data center. Each agency shall submit the
2362 plan by October 15 of each year to DIGIT, the Office of Policy
2363 and Budget in the Executive Office of the Governor, and the
2364 chairs of the legislative appropriations committees, and the
2365 Northwest Regional Data Center. For each application, the plan
2366 must identify and document the readiness, appropriate strategy,
2367 and high-level timeline for transition to a cloud-computing
2368 service based on the application's quality, cost, and resource
2369 requirements. This information must be used to assist the state
2370 data center in making adjustments to its service offerings.

2371 Section 22. Section 1004.649, Florida Statutes, is amended
2372 to read:

2373 1004.649 Northwest Regional Data Center.—There is created
2374 at Florida State University the Northwest Regional Data Center.
2375 The data center shall serve as the state data center as
2376 designated in s. 282.201

2377 (1) For the purpose of providing data center services to
2378 its state agency customers, the Northwest Regional Data Center

31-01058B-26

2026480

2379 is designated as a state data center for all state agencies and
2380 shall:

2381 (a) Operate under a governance structure that represents
2382 its customers proportionally.

2383 (b) Maintain an appropriate cost allocation methodology
2384 that accurately bills state agency customers based solely on the
2385 actual direct and indirect costs of the services provided to
2386 state agency customers and ensures that, for any fiscal year,
2387 state agency customers are not subsidizing other customers of
2388 the data center. Such cost allocation methodology must comply
2389 with applicable state and federal regulations concerning the
2390 distribution and use of state and federal funds.

2391 (c) Enter into a service level agreement with each state
2392 agency customer to provide services as defined and approved by
2393 the governing board of the center. At a minimum, such service-
2394 level agreements must:

2395 1. Identify the parties and their roles, duties, and
2396 responsibilities under the agreement;

2397 2. State the duration of the agreement term, which may not
2398 exceed 3 years, and specify the conditions for up to two
2399 optional 1-year renewals of the agreement before execution of a
2400 new agreement;

2401 3. Identify the scope of work;

2402 4. Establish the services to be provided, the business
2403 standards that must be met for each service, the cost of each
2404 service, and the process by which the business standards for
2405 each service are to be objectively measured and reported;

2406 5. Provide a timely billing methodology for recovering the
2407 cost of services provided pursuant to s. 215.422;

31-01058B-26

2026480

2408 6. Provide a procedure for modifying the service level
2409 agreement to address any changes in projected costs of service;

2410 7. Include a right-to-audit clause to ensure that the
2411 parties to the agreement have access to records for audit
2412 purposes during the term of the service level agreement;

2413 8. Identify the products or services to be delivered with
2414 sufficient specificity to permit an external financial or
2415 performance audit;

2416 9. Provide that the service level agreement may be
2417 terminated by either party for cause only after giving the other
2418 party notice in writing of the cause for termination and an
2419 opportunity for the other party to resolve the identified cause
2420 within a reasonable period; and

2421 10. Provide state agency customer entities with access to
2422 applications, servers, network components, and other devices
2423 necessary for entities to perform business activities and
2424 functions and as defined and documented in a service level
2425 agreement.

2426 (d) In its procurement process, show preference for cloud-
2427 computing solutions that minimize or do not require the
2428 purchasing or financing of state data center infrastructure,
2429 that meet the needs of state agency customer entities, that
2430 reduce costs, and that meet or exceed the applicable state and
2431 federal laws, regulations, and standards for cybersecurity.

2432 (e) Assist state agency customer entities in transitioning
2433 from state data center services to other third party cloud-
2434 computing services procured by a customer entity or by the
2435 Northwest Regional Data Center on behalf of the customer entity.

2436 (f) Provide to the Board of Governors the total annual

31-01058B-26

2026480

2437 budget by major expenditure category, including, but not limited
2438 to, salaries, expenses, operating capital outlay, contracted
2439 services, or other personnel services by July 30 each fiscal
2440 year.

2441 (g) Provide to each state agency customer its projected
2442 annual cost for providing the agreed upon data center services
2443 by September 1 each fiscal year.

2444 (h) Provide a plan for consideration by the Legislative
2445 Budget Commission if the governing body of the center approves
2446 the use of a billing rate schedule after the start of the fiscal
2447 year that increases any state agency customer's costs for that
2448 fiscal year.

2449 (i) Provide data center services that comply with
2450 applicable state and federal laws, regulations, and policies,
2451 including all applicable security, privacy, and auditing
2452 requirements.

2453 (j) Maintain performance of the data center facilities by
2454 ensuring proper data backup; data backup recovery; disaster
2455 recovery; and appropriate security, power, cooling, fire
2456 suppression, and capacity.

2457 (k) Prepare and submit state agency customer invoices to
2458 the Department of Management Services for approval. Upon
2459 approval or by default pursuant to s. 282.201(5), submit
2460 invoices to state agency customers.

2461 (l) As funded in the General Appropriations Act, provide
2462 data center services to state agencies from multiple facilities.

2463 (2) Unless exempt from the requirement to use the state
2464 data center pursuant to s. 282.201(2) or as authorized by the
2465 Legislature, a state agency may not do any of the following:

31-01058B-26

2026480

2466 (a) Terminate services with the Northwest Regional Data
2467 Center without giving written notice of intent to terminate
2468 services 180 days before such termination.

2469 (b) Procure third-party cloud computing services without
2470 evaluating the cloud computing services provided by the
2471 Northwest Regional Data Center.

2472 (c) Exceed 30 days from receipt of approved invoices to
2473 remit payment for state data center services provided by the
2474 Northwest Regional Data Center.

2475 (3) The Northwest Regional Data Center's authority to
2476 provide data center services to its state agency customers may
2477 be terminated if:

2478 (a) The center requests such termination to the Board of
2479 Governors, the President of the Senate, and the Speaker of the
2480 House of Representatives; or

2481 (b) The center fails to comply with the provisions of this
2482 section.

2483 (4) The Northwest Regional Data Center is the lead entity
2484 responsible for creating, operating, and managing, including the
2485 research conducted by, the Florida Behavioral Health Care Data
2486 Repository as established by this subsection.

2487 (a) The purpose of the data repository is to create a
2488 centralized system for:

2489 1. Collecting and analyzing existing statewide behavioral
2490 health care data to:

2491 a. Better understand the scope of and trends in behavioral
2492 health services, spending, and outcomes to improve patient care
2493 and enhance the efficiency and effectiveness of behavioral
2494 health services;

31-01058B-26

2026480

2495 b. Better understand the scope of, trends in, and
2496 relationship between behavioral health, criminal justice,
2497 incarceration, and the use of behavioral health services as a
2498 diversion from incarceration for individuals with mental
2499 illness; and

2500 c. Enhance the collection and coordination of treatment and
2501 outcome information as an ongoing evidence base for research and
2502 education related to behavioral health.

2503 2. Developing useful data analytics, economic metrics, and
2504 visual representations of such analytics and metrics to inform
2505 relevant state agencies and the Legislature of data and trends
2506 in behavioral health.

2507 (b) The Northwest Regional Data Center shall develop, in
2508 collaboration with the Data Analysis Committee of the Commission
2509 on Mental Health and Substance Use Disorder created under s.
2510 394.9086 and with relevant stakeholders, a plan that includes
2511 all of the following:

2512 1. A project plan that describes the technology,
2513 methodology, timeline, cost, and resources necessary to create a
2514 centralized, integrated, and coordinated data system.

2515 2. A proposed governance structure to oversee the
2516 implementation and operations of the repository.

2517 3. An integration strategy to incorporate existing data
2518 from relevant state agencies, including, but not limited to, the
2519 Agency for Health Care Administration, the Department of
2520 Children and Families, the Department of Juvenile Justice, the
2521 Office of the State Courts Administrator, and the Department of
2522 Corrections.

2523 4. Identification of relevant data and metrics to support

31-01058B-26

2026480

2524 actionable information and ensure the efficient and responsible
2525 use of taxpayer dollars within behavioral health systems of
2526 care.

2527 5. Data security requirements for the repository.

2528 6. The structure and process that will be used to create an
2529 annual analysis and report that gives state agencies and the
2530 Legislature a better general understanding of trends and issues
2531 in the state's behavioral health systems of care and the trends
2532 and issues in behavioral health systems related to criminal
2533 justice treatment, diversion, and incarceration.

2534 (e) By December 1, 2025, the Northwest Regional Data
2535 Center, in collaboration with the Data Analysis Committee of the
2536 Commission on Mental Health and Substance Use Disorder, shall
2537 submit the developed plan for implementation and ongoing
2538 operation with a proposed budget to the Governor, the President
2539 of the Senate, and the Speaker of the House of Representatives
2540 for review.

2541 (d) Beginning December 1, 2026, and annually thereafter,
2542 the Northwest Regional Data Center shall submit the developed
2543 trends and issues report under subparagraph (b) 6. to the
2544 Governor, the President of the Senate, and the Speaker of the
2545 House of Representatives.

2546 (5) If such authority is terminated, the center has 1 year
2547 to provide for the transition of its state agency customers to a
2548 qualified alternative cloud-based data center that meets the
2549 enterprise architecture standards established by the Florida
2550 Digital Service.

2551 Section 23. Subsection (2) of section 20.22, Florida
2552 Statutes, is amended to read:

31-01058B-26

2026480

2553 20.22 Department of Management Services.—There is created a
2554 Department of Management Services.

2555 (2) The following divisions, programs, and services within
2556 the Department of Management Services are established:

2557 (a) Facilities Program.

2558 (b) ~~The Florida Digital Service.~~

2559 (e) Workforce Program.

2560 (c) 1. ~~(d)~~ Support Program.

2561 2. Federal Property Assistance Program.

2562 (d) ~~(e)~~ Administration Program.

2563 (e) ~~(f)~~ Division of Administrative Hearings.

2564 (f) ~~(g)~~ Division of Retirement.

2565 (g) ~~(h)~~ Division of State Group Insurance.

2566 (h) ~~(i)~~ Division of Telecommunications.

2567 Section 24. Subsections (1), (5), (7), and (8) of section
2568 282.802, Florida Statutes, are amended to read:

2569 282.802 Government Technology Modernization Council.—

2570 (1) The Government Technology Modernization Council, an
2571 advisory council as defined in s. 20.03(7), is located ~~created~~
2572 within DIGIT ~~the department~~. Except as otherwise provided in
2573 this section, the advisory council shall operate in a manner
2574 consistent with s. 20.052.

2575 (5) The state chief information officer ~~Secretary of~~
2576 ~~Management Services~~, or his or her designee, shall serve as the
2577 ex officio, nonvoting executive director of the council.

2578 (7) ~~(a)~~ The council shall meet at least quarterly to:

2579 (a)1. Recommend legislative and administrative actions that
2580 the Legislature and state agencies as defined in s. 282.0041 ~~s.~~
2581 ~~282.318(2)~~ may take to promote the development of data

31-01058B-26

2026480

2582 modernization in this state.

2583 (b) 2. Assess and provide guidance on necessary legislative
2584 reforms and the creation of a state code of ethics for
2585 artificial intelligence systems in state government.

2586 (c) 3. Assess the effect of automated decision systems or
2587 identity management on constitutional and other legal rights,
2588 duties, and privileges of residents of this state.

2589 (d) 4. Evaluate common standards for artificial intelligence
2590 safety and security measures, including the benefits of
2591 requiring disclosure of the digital provenance for all images
2592 and audio created using generative artificial intelligence as a
2593 means of revealing the origin and edit of the image or audio, as
2594 well as the best methods for such disclosure.

2595 (e) 5. Assess the manner in which governmental entities and
2596 the private sector are using artificial intelligence with a
2597 focus on opportunity areas for deployments in systems across
2598 this state.

2599 (f) 6. Determine the manner in which artificial intelligence
2600 is being exploited by bad actors, including foreign countries of
2601 concern as defined in s. 287.138(1).

2602 (g) 7. Evaluate the need for curriculum to prepare school-
2603 age audiences with the digital media and visual literacy skills
2604 needed to navigate the digital information landscape.

2605 (b) ~~At least one quarterly meeting of the council must be a~~
2606 ~~joint meeting with the Florida Cybersecurity Advisory Council.~~

2607 (8) ~~By December 31, 2024, and Each December 31 thereafter,~~
2608 the council shall submit to the Governor, the Commissioner of
2609 Agriculture, the Chief Financial Officer, the Attorney General,
2610 the President of the Senate, and the Speaker of the House of

31-01058B-26

2026480

2611 Representatives any legislative recommendations considered
2612 necessary by the council to modernize government technology,
2613 including:

2614 (a) Recommendations for policies necessary to:

2615 1. Accelerate adoption of technologies that will increase
2616 productivity of state enterprise information technology systems,
2617 improve customer service levels of government, and reduce
2618 administrative or operating costs.

2619 2. Promote the development and deployment of artificial
2620 intelligence systems, financial technology, education
2621 technology, or other enterprise management software in this
2622 state.

2623 3. Protect Floridians from bad actors who use artificial
2624 intelligence.

2625 (b) Any other information the council considers relevant.

2626 Section 25. Section 282.604, Florida Statutes, is amended
2627 to read:

2628 282.604 Adoption of rules.—~~DIGIT The Department of~~
2629 ~~Management Services~~ shall, with input from stakeholders, adopt
2630 rules pursuant to ss. 120.536(1) and 120.54 for the development,
2631 procurement, maintenance, and use of accessible electronic
2632 information technology by governmental units.

2633 Section 26. Subsection (4) of section 287.0591, Florida
2634 Statutes, is amended to read:

2635 287.0591 Information technology; vendor disqualification.—

2636 (4) If the department issues a competitive solicitation for
2637 information technology commodities, consultant services, or
2638 staff augmentation contractual services, the state chief
2639 information officer must Florida Digital Service within the

31-01058B-26

2026480

2640 ~~department~~ shall participate in such solicitations.

2641 Section 27. Paragraph (b) of subsection (4) of section
2642 443.1113, Florida Statutes, is amended to read:

2643 443.1113 Reemployment Assistance Claims and Benefits
2644 Information System.—

2645 (4)

2646 (b) The department shall seek input on recommended
2647 enhancements from, at a minimum, the following entities:

2648 1. The Division of Integrated Government Innovation and
2649 ~~Technology Florida Digital Service within the Department of~~
2650 ~~Management Services~~.

2651 2. The General Tax Administration Program Office within the
2652 Department of Revenue.

2653 3. The Division of Accounting and Auditing within the
2654 Department of Financial Services.

2655 Section 28. Subsection (5) of section 943.0415, Florida
2656 Statutes, is amended to read:

2657 943.0415 Cybercrime Office.—There is created within the
2658 Department of Law Enforcement the Cybercrime Office. The office
2659 may:

2660 (5) Consult with the state chief information security
2661 officer of the Division of Integrated Government Innovation and
2662 ~~Technology Florida Digital Service within the Department of~~
2663 ~~Management Services~~ in the adoption of rules relating to the
2664 information technology security provisions in s. 282.318.

2665 Section 29. Subsection (3) of section 1004.444, Florida
2666 Statutes, is amended to read:

2667 1004.444 Florida Center for Cybersecurity.—

2668 (3) Upon receiving a request for assistance from a ~~the~~

31-01058B-26

2026480

2669 ~~Department of Management Services, the Florida Digital Service,~~
2670 ~~or another~~ state agency, the center is authorized, but may not
2671 be compelled by the agency, to conduct, consult on, or otherwise
2672 assist any state-funded initiatives related to:

2673 (a) Cybersecurity training, professional development, and
2674 education for state and local government employees, including
2675 school districts and the judicial branch; and

2676 (b) Increasing the cybersecurity effectiveness of the
2677 state's and local governments' technology platforms and
2678 infrastructure, including school districts and the judicial
2679 branch.

2680 Section 30. This act shall take effect January 5, 2027.