By the Committee on Appropriations

576-02644-25 20257026 1 A bill to be entitled 2 An act relating to information technology; creating s. 3 20.70, F.S.; creating the Agency for State Systems and 4 Enterprise Technology (ASSET); providing that the 5 Governor and Cabinet are the head of the agency; establishing divisions and offices of the agency; 6 7 providing for an executive director of the agency; 8 providing that the executive director also serves as 9 the state chief information officer; providing for the 10 appointment and removal of such executive director; 11 prohibiting the state chief information officer from 12 having financial, personal, or business conflicts of 13 interest related to certain vendors, contractors, and service providers of the state; requiring that the 14 state chief information officer selection committee 15 16 within ASSET be appointed and provide a specified 17 number of nominees upon a vacancy of such officer; 18 providing the composition of such committee; requiring 19 that a member of the committee designate an alternate 20 state agency chief information officer to serve on the 21 committee under a specified circumstance; providing 22 the qualifications for the state chief information 23 officer; providing that persons who currently serve, 24 or have served, as state agency heads are ineligible to serve as the state chief information officer; 25 transferring the state chief information officer of 2.6 27 the Department of Management Services to ASSET until 28 the Governor and the Cabinet appoint a permanent 29 officer; requiring that such appointment occur by a

Page 1 of 111

576-02644-25 20257026 30 specified date; amending s. 97.0525, F.S.; requiring that the Division of Elections comprehensive risk 31 32 assessment comply with the risk assessment methodology developed by ASSET; amending s. 112.22, F.S.; defining 33 34 the term "ASSET"; deleting the term "department"; 35 revising the definition of the term "prohibited 36 application"; authorizing public employers to request 37 a certain waiver from ASSET; requiring ASSET to take specified actions; deleting obsolete language; 38 39 requiring ASSET to adopt rules; amending s. 119.0725, 40 F.S.; providing that confidential and exempt 41 information must be made available to ASSET; amending s. 216.023, F.S.; requiring agencies and the judicial 42 branch to include a cumulative inventory and a certain 43 44 status report of specified projects with their legislative budget requests; defining the term 45 46 "technology-related project"; deleting a provision 47 requiring state agencies and the judicial branch to include a cumulative inventory and a certain status 48 49 report of specified projects as part of a budget 50 request; conforming a cross-reference; amending s. 282.0041, F.S.; deleting and revising definitions; 51 defining the terms "ASSET" and "technical debt"; 52 53 amending s. 282.0051, F.S.; deleting obsolete 54 language; revising the powers, duties, and functions of the Department of Management Services, through the 55 56 Florida Digital Service; deleting a requirement that 57 the state chief information officer, in consultation 58 with the Secretary of Management Services, designate a

Page 2 of 111

576-02644-25 20257026 59 state chief data officer; deleting requirements of the 60 department, acting through the Florida Digital 61 Service, relating to the use of appropriated funds for certain actions; deleting provisions related to 62 63 information technology projects that have a total 64 project cost in excess of \$10 million; providing for 65 the future repeal of the section; deleting a requirement to adopt rules; repealing s. 282.00515, 66 F.S., relating to duties of Cabinet agencies; creating 67 68 s. 282.006, F.S.; requiring ASSET to operate as the 69 state enterprise organization for information 70 technology governance and as the lead entity 71 responsible for understanding needs and environments, 72 creating standards and strategy, supporting state 73 agency technology efforts, and reporting on the state 74 of information technology in this state; providing 75 legislative intent; requiring ASSET to establish the 76 strategic direction of information technology in the 77 state; requiring ASSET to develop and publish 78 information technology policy for a specified purpose; 79 requiring that such policy be updated as necessary to 80 meet certain requirements and advancements in 81 technology; requiring ASSET to take specified actions 82 related to oversight of the state's technology 83 enterprise; requiring ASSET to produce specified reports, recommendations, and analyses and provide 84 85 such reports, recommendations, and analyses to the 86 Governor, the Commissioner of Agriculture, the Chief 87 Executive Officer, the Attorney General, and the

Page 3 of 111

116

576-02644-25 20257026 88 Legislature by specified dates and at specified 89 intervals; providing requirements for such reports; 90 requiring ASSET to conduct a market analysis at a 91 certain interval beginning on a specified date; 92 providing requirements for the market analysis; 93 requiring that each market analysis be used to prepare 94 a strategic plan for specified purposes; requiring 95 that copies of the market analysis and strategic plan be submitted by a specified date; authorizing ASSET to 96 adopt rules; creating s. 282.0061, F.S.; providing 97 98 legislative intent; requiring ASSET to complete a 99 certain full baseline needs assessment of state 100 agencies, develop a specified plan to conduct such 101 assessments, and submit such plan to the Governor, the 102 Commissioner of Agriculture, the Chief Financial 103 Officer, the Attorney General, and the Legislature 104 within a specified timeframe; requiring ASSET to 105 support state agency strategic planning efforts and 106 assist such agencies with a certain phased roadmap; 107 providing requirements for such roadmaps; requiring 108 ASSET to make recommendations for standardizing data 109 across state agencies for a specified purpose and identify any opportunities for standardization and 110 111 consolidation of information technology services 112 across state agencies and support specified functions; 113 requiring ASSET to develop standards for use by state 114 agencies and enforce consistent standards and promote 115 best practices across all state agencies; requiring

Page 4 of 111

CODING: Words stricken are deletions; words underlined are additions.

ASSET to provide a certain report to the Governor, the

145

576-02644-25 20257026 117 Commissioner of Agriculture, the Chief Financial 118 Officer, the Attorney General, and the Legislature by 119 a specified date; providing requirements of the 120 report; providing the duties and responsibilities of 121 ASSET related to state agency technology projects; 122 requiring ASSET, in consultation with state agencies, 123 to create a methodology, approach, and applicable 124 templates and formats for identifying and collecting 125 information technology expenditure data at the state 126 agency level; requiring ASSET to obtain, review, and 127 maintain records of the appropriations, expenditures, 128 and revenues for information technology for each state 129 agency; requiring ASSET to prescribe the format for 130 state agencies to provide financial information to 131 ASSET for inclusion in a certain annual report; 132 requiring state agencies to submit such information by 133 a specified date annually; requiring that such 134 information be reported to ASSET to determine all 135 costs and expenditures of information technology 136 assets and resources provided to state agencies; 137 requiring ASSET to work with state agencies to provide 138 alternative standards, policies, or requirements under 139 specified circumstances; creating s. 282.0062, F.S.; 140 establishing workgroups within ASSET to facilitate 141 coordination with state agencies; providing for the 142 membership and duties of such workgroups; creating s. 143 282.0063, F.S.; requiring ASSET to perform specified 144 actions to develop and manage career paths,

Page 5 of 111

progressions, and training programs for the benefit of

CODING: Words stricken are deletions; words underlined are additions.

174

576-02644-25 20257026 146 state agency personnel; creating s. 282.0064, F.S.; 147 requiring ASSET, in coordination with the Department 148 of Management Services, to establish a policy for all information technology-related solicitations, 149 150 contracts, and procurements; providing requirements 151 for the policy related to state term contracts, all 152 contracts, and information technology projects that 153 require oversight; prohibiting entities providing 154 independent verification and validation from having 155 certain interests, responsibilities, or other 156 participation in the project; providing the primary 157 objective of independent verification and validation; 158 requiring the entity performing such verification and 159 validation to provide specified regular reports and 160 assessments; requiring the Division of State 161 Purchasing within the Department of Management Services to coordinate with ASSET on state term 162 163 contract solicitations and invitations to negotiate; 164 requiring ASSET to evaluate vendor responses and 165 answer vendor questions on such solicitations and 166 invitations; creating s. 282.0065, F.S.; requiring 167 ASSET to establish, maintain, and manage a certain 168 test laboratory, beginning at a specified time; 169 providing the purpose of the laboratory; requiring 170 ASSET to take specified actions relating to the 171 laboratory; creating s. 282.0066, F.S.; requiring 172 ASSET to develop, implement, and maintain a certain 173 library; providing requirements for the library;

Page 6 of 111

requiring ASSET to establish procedures that ensure

576-02644-25

20257026

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

Page 7 of 111

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

Cybersecurity Operations Center, to notify the

576-02644-25

204

221

231

232

20257026

Page 8 of 111

chief information technology procurement officer,

establish specified procedures for procuring

576-02644-25

20257026

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

Page 9 of 111

576-02644-25 20257026 262 Agriculture, the Chief Financial Officer, the Attorney 263 General, and the Legislature; conforming provisions to 264 changes made by the act; requiring the state chief 265 information security officer to establish certain 266 guidelines and processes by a specified date; 267 conforming cross-references; repealing s. 282.319, 268 F.S., relating to the Florida Cybersecurity Advisory 269 Council; establishing positions within ASSET; 270 establishing the Division of Enterprise Information 271 Technology Services and the Division of Enterprise Information Technology Purchasing and associated 272 273 bureaus; providing the responsibilities of the 274 bureaus; establishing the chief information officer 275 policy workgroup; providing the membership, purpose, 276 chair, and duties of the workgroup; providing for the 277 expiration of the workgroup upon completion of its 278 duties; amending s. 282.201, F.S.; establishing the 279 state data center within the Northwest Regional Data 280 Center; requiring the Northwest Regional Data Center 281 to meet or exceed specified information technology 282 standards; revising requirements of the state data 283 center; abrogating the scheduled repeal of the 284 Division of Emergency Management's exemption from 285 using the state data center; deleting Department of 286 Management Services' responsibilities related to the 287 state data center; deleting provisions relating to 288 contracting with the Northwest Regional Data Center; 289 creating s. 282.0211, F.S.; designating the Northwest 290 Regional Data Center as a state data center for all

SB 7026

Page 10 of 111

	576-02644-25 20257026
291	state agencies; requiring the data center to engage in
292	specified actions; prohibiting state agencies from
293	terminating services with the data center without
294	giving written notice within a specified timeframe,
295	procuring third-party cloud-computing services without
296	evaluating the data center's cloud-computing services,
297	and exceeding a specified timeframe to remit payments
298	for data center services provided by the data center;
299	specifying circumstances under which the data center's
300	designation may be terminated; providing that the data
301	center has a specified timeframe to provide for the
302	transition of state agency customers to a qualified
303	alternative cloud-based data center that meets
304	specified standards; amending s. 1004.649, F.S.;
305	creating the Northwest Regional Data Center at Florida
306	State University; conforming provisions to changes
307	made by the act; amending s. 20.22, F.S.; deleting the
308	Florida Digital Service from the list of divisions,
309	programs, and services of the Department of Management
310	Services; amending s. 282.802, F.S.; providing that
311	the Government Technology Modernization Council is
312	located within ASSET; providing that the state chief
313	information officer, or his or her designee, is the ex
314	officio executive director of the council; conforming
315	provisions to changes made by the act; requiring the
316	council annually to submit to the Commissioner of
317	Agriculture, the Chief Financial Officer, and the
318	Attorney General certain legislative recommendations;
319	amending s. 282.604, F.S.; requiring ASSET, with input

Page 11 of 111

320from stakeholders, to adopt rules; amending s.321287.0591, F.S.; requiring the state chief information322officer, instead of the Florida Digital Service, to323participate in certain solicitations; amending s.324288.012, F.S.; conforming a cross-reference; amending325s. 443.1113, F.S.; requiring the Department of326Commerce to seek input on recommended enhancements327from ASSET instead of the Florida Digital Service;328amending s. 943.0415, F.S.; authorizing the Cybercrime329Office to consult with the state chief information330security officer of ASSET instead of the Florida331Digital Service; amending s. 1004.444, F.S.;332authorizing the Florida Center for Cybersecurity to333conduct, consult, or assist state agencies upon334receiving a request for assistance from such agencies;335providing effective dates.336Section 1. Section 20.70, Florida Statutes, is created to34120.70 Agency for State Systems and Enterprise Technology342There is created the Agency for State Systems and Enterprise343Technology. The head of the agency is the Governor and Cabinet.344(1) DIVISION AND OFFICESThe following divisions and345offices of the Agency for State Systems and Enterprise346Technology are established:347(a) The Division of Administrative Services.348(b) The Office of Information Technology.		576-02644-25 20257026
322officer, instead of the Florida Digital Service, to323participate in certain solicitations; amending s.324288.012, F.S.; conforming a cross-reference; amending325s. 443.1113, F.S.; requiring the Department of326Commerce to seek input on recommended enhancements327from ASSET instead of the Florida Digital Service;328amending s. 943.0415, F.S.; authorizing the Cybercrime329Office to consult with the state chief information330security officer of ASSET instead of the Florida331Digital Service; amending s. 1004.444, F.S.;332authorizing the Florida Center for Cybersecurity to333conduct, consult, or assist state agencies upon334receiving a request for assistance from such agencies;335providing effective dates.336Section 1. Section 20.70, Florida Statutes, is created to34120.70 Agency for State Systems and Enterprise Technology342There is created the Agency for State Systems and Enterprise343offices of the Agency for State Systems and Enterprise344(1) DIVISIONS AND OFFICESThe following divisions and345offices of the Agency for State Systems and Enterprise346Technology are established:347(a) The Division of Administrative Services.	320	from stakeholders, to adopt rules; amending s.
323participate in certain solicitations; amending s.324288.012, F.S.; conforming a cross-reference; amending325s. 443.1113, F.S.; requiring the Department of326Commerce to seek input on recommended enhancements327from ASSET instead of the Florida Digital Service;328amending s. 943.0415, F.S.; authorizing the Cybercrime329Office to consult with the state chief information330security officer of ASSET instead of the Florida331Digital Service; amending s. 1004.444, F.S.;332authorizing the Florida Center for Cybersecurity to333conduct, consult, or assist state agencies upon334receiving a request for assistance from such agencies;335providing effective dates.336Section 1. Section 20.70, Florida Statutes, is created to34120.70 Agency for State Systems and Enterprise343There is created the Agency for State Systems and Enterprise344(1) DIVISIONS AND OFFICESThe following divisions and345offices of the Agency for State Systems and Enterprise346Technology are established:347(a) The Division of Administrative Services.	321	287.0591, F.S.; requiring the state chief information
228.012, F.S.; conforming a cross-reference; amending325s. 443.1113, F.S.; requiring the Department of326Commerce to seek input on recommended enhancements327from ASSET instead of the Florida Digital Service;328amending s. 943.0415, F.S.; authorizing the Cybercrime329Office to consult with the state chief information330security officer of ASSET instead of the Florida331Digital Service; amending s. 1004.444, F.S.;332authorizing the Florida Center for Cybersecurity to333conduct, consult, or assist state agencies upon334receiving a request for assistance from such agencies;335providing effective dates.336Section 1. Section 20.70, Florida Statutes, is created to34120.70 Agency for State Systems and Enterprise Technology342There is created the Agency for State Systems and Enterprise343Gffices of the Agency for State Systems and Enterprise344(1) DIVISIONS AND OFFICESThe following divisions and345offices of the Agency for State Systems and Enterprise346Technology are established:347(a) The Division of Administrative Services.	322	officer, instead of the Florida Digital Service, to
 s. 443.1113, F.S.; requiring the Department of Commerce to seek input on recommended enhancements from ASSET instead of the Florida Digital Service; amending s. 943.0415, F.S.; authorizing the Cybercrime Office to consult with the state chief information security officer of ASSET instead of the Florida Digital Service; amending s. 1004.444, F.S.; authorizing the Florida Center for Cybersecurity to conduct, consult, or assist state agencies upon receiving a request for assistance from such agencies; providing effective dates. Be It Enacted by the Legislature of the State of Florida: 20.70 Agency for State Systems and Enterprise Technology There is created the Agency for State Systems and Enterprise Technology. The head of the agency is the Governor and Cabinet. (1) DIVISIONS AND OFFICESThe following divisions and offices of the Agency for State Systems and Enterprise Technology are established: (a) The Division of Administrative Services. 	323	participate in certain solicitations; amending s.
326Commerce to seek input on recommended enhancements327from ASSET instead of the Florida Digital Service;328amending s. 943.0415, F.S.; authorizing the Cybercrime329Office to consult with the state chief information330security officer of ASSET instead of the Florida331Digital Service; amending s. 1004.444, F.S.;332authorizing the Florida Center for Cybersecurity to333conduct, consult, or assist state agencies upon344receiving a request for assistance from such agencies;355providing effective dates.366377378Be It Enacted by the Legislature of the State of Florida:389Section 1. Section 20.70, Florida Statutes, is created to340read:341 <u>20.70 Agency for State Systems and Enterprise Technology</u> 342There is created the Agency for State Systems and Enterprise343Technology. The head of the agency is the Governor and Cabinet.344(1) DIVISIONS AND OFFICESThe following divisions and345offices of the Agency for State Systems and Enterprise346Technology are established:347(a) The Division of Administrative Services.	324	288.012, F.S.; conforming a cross-reference; amending
327from ASSET instead of the Florida Digital Service;328amending s. 943.0415, F.S.; authorizing the Cybercrime329Office to consult with the state chief information330security officer of ASSET instead of the Florida331Digital Service; amending s. 1004.444, F.S.;332authorizing the Florida Center for Cybersecurity to333conduct, consult, or assist state agencies upon344receiving a request for assistance from such agencies;355providing effective dates.366377378Be It Enacted by the Legislature of the State of Florida:388section 1. Section 20.70, Florida Statutes, is created to340read:34120.70 Agency for State Systems and Enterprise Technology342There is created the Agency for State Systems and Enterprise343Technology. The head of the agency is the Governor and Cabinet.344(1) DIVISIONS AND OFFICESThe following divisions and345offices of the Agency for State Systems and Enterprise346Technology are established:347(a) The Division of Administrative Services.	325	s. 443.1113, F.S.; requiring the Department of
328amending s. 943.0415, F.S.; authorizing the Cybercrime329Office to consult with the state chief information330security officer of ASSET instead of the Florida331Digital Service; amending s. 1004.444, F.S.;332authorizing the Florida Center for Cybersecurity to333conduct, consult, or assist state agencies upon344receiving a request for assistance from such agencies;355providing effective dates.36637737Be It Enacted by the Legislature of the State of Florida:388section 1. Section 20.70, Florida Statutes, is created to340read:34120.70 Agency for State Systems and Enterprise Technology342There is created the Agency for State Systems and Enterprise343Technology. The head of the agency is the Governor and Cabinet.344(1) DIVISIONS AND OFFICESThe following divisions and345offices of the Agency for State Systems and Enterprise346Technology are established:347(a) The Division of Administrative Services.	326	Commerce to seek input on recommended enhancements
329Office to consult with the state chief information330security officer of ASSET instead of the Florida331Digital Service; amending s. 1004.444, F.S.;332authorizing the Florida Center for Cybersecurity to333conduct, consult, or assist state agencies upon344receiving a request for assistance from such agencies;355providing effective dates.36633737Be It Enacted by the Legislature of the State of Florida:38section 1. Section 20.70, Florida Statutes, is created to39read:34120.70 Agency for State Systems and Enterprise Technology342There is created the Agency for State Systems and Enterprise343Technology. The head of the agency is the Governor and Cabinet.344(1) DIVISIONS AND OFFICESThe following divisions and345offices of the Agency for State Systems and Enterprise346Technology are established:347(a) The Division of Administrative Services.	327	from ASSET instead of the Florida Digital Service;
 330 security officer of ASSET instead of the Florida 331 Digital Service; amending s. 1004.444, F.S.; 332 authorizing the Florida Center for Cybersecurity to 333 conduct, consult, or assist state agencies upon 334 receiving a request for assistance from such agencies; 335 providing effective dates. 336 337 Be It Enacted by the Legislature of the State of Florida: 338 339 Section 1. Section 20.70, Florida Statutes, is created to 340 read: 341 <u>20.70 Agency for State Systems and Enterprise Technology</u> 342 <u>There is created the Agency for State Systems and Enterprise</u> 343 <u>offices of the Agency for State Systems and Enterprise</u> 344 <u>(1) DIVISIONS AND OFFICESThe following divisions and</u> 345 <u>offices of the Agency for State Systems and Enterprise</u> 346 <u>Technology are established:</u> 347 <u>(a) The Division of Administrative Services.</u> 	328	amending s. 943.0415, F.S.; authorizing the Cybercrime
331Digital Service; amending s. 1004.444, F.S.;332authorizing the Florida Center for Cybersecurity to333conduct, consult, or assist state agencies upon334receiving a request for assistance from such agencies;335providing effective dates.336337Be It Enacted by the Legislature of the State of Florida:338339Section 1. Section 20.70, Florida Statutes, is created to34120.70 Agency for State Systems and Enterprise Technology342There is created the Agency for State Systems and Enterprise343Technology. The head of the agency is the Governor and Cabinet.344(1) DIVISIONS AND OFFICESThe following divisions and345offices of the Agency for State Systems and Enterprise346Technology are established:347(a) The Division of Administrative Services.	329	Office to consult with the state chief information
 authorizing the Florida Center for Cybersecurity to conduct, consult, or assist state agencies upon receiving a request for assistance from such agencies; providing effective dates. Be It Enacted by the Legislature of the State of Florida: section 1. Section 20.70, Florida Statutes, is created to read: <u>20.70 Agency for State Systems and Enterprise Technology</u> <u>There is created the Agency for State Systems and Enterprise</u> <u>Technology. The head of the agency is the Governor and Cabinet.</u> <u>offices of the Agency for State Systems and Enterprise</u> <u>Technology are established:</u> <u>(a) The Division of Administrative Services.</u> 	330	security officer of ASSET instead of the Florida
333 conduct, consult, or assist state agencies upon 334 receiving a request for assistance from such agencies; 335 providing effective dates. 336 337 Be It Enacted by the Legislature of the State of Florida: 338 339 Section 1. Section 20.70, Florida Statutes, is created to 340 read: 341 <u>20.70 Agency for State Systems and Enterprise Technology</u> 342 There is created the Agency for State Systems and Enterprise 343 <u>Technology. The head of the agency is the Governor and Cabinet.</u> 344 <u>(1) DIVISIONS AND OFFICESThe following divisions and 345 offices of the Agency for State Systems and Enterprise 346 <u>Technology are established:</u> 347 <u>(a) The Division of Administrative Services.</u></u>	331	Digital Service; amending s. 1004.444, F.S.;
<pre>334 receiving a request for assistance from such agencies; 335 providing effective dates. 336 337 Be It Enacted by the Legislature of the State of Florida: 338 339 Section 1. Section 20.70, Florida Statutes, is created to 340 read: 341 <u>20.70 Agency for State Systems and Enterprise Technology</u> 342 There is created the Agency for State Systems and Enterprise 343 <u>Technology. The head of the agency is the Governor and Cabinet.</u> 344 <u>(1) DIVISIONS AND OFFICESThe following divisions and 345 offices of the Agency for State Systems and Enterprise 346 <u>Technology are established:</u> 347 <u>(a) The Division of Administrative Services.</u></u></pre>	332	authorizing the Florida Center for Cybersecurity to
335 providing effective dates. 336 337 Be It Enacted by the Legislature of the State of Florida: 338 339 Section 1. Section 20.70, Florida Statutes, is created to 340 read: 341 <u>20.70 Agency for State Systems and Enterprise Technology</u> 342 <u>There is created the Agency for State Systems and Enterprise</u> 343 <u>Technology. The head of the agency is the Governor and Cabinet.</u> 344 <u>(1) DIVISIONS AND OFFICESThe following divisions and</u> 345 <u>offices of the Agency for State Systems and Enterprise</u> 346 <u>Technology are established:</u> 347 <u>(a) The Division of Administrative Services.</u>	333	conduct, consult, or assist state agencies upon
Be It Enacted by the Legislature of the State of Florida: Be It Enacted by the Legislature of the State of Florida: Section 1. Section 20.70, Florida Statutes, is created to read: 20.70 Agency for State Systems and Enterprise Technology There is created the Agency for State Systems and Enterprise Technology. The head of the agency is the Governor and Cabinet. (1) DIVISIONS AND OFFICESThe following divisions and offices of the Agency for State Systems and Enterprise Technology are established: (a) The Division of Administrative Services.	334	receiving a request for assistance from such agencies;
 Be It Enacted by the Legislature of the State of Florida: Section 1. Section 20.70, Florida Statutes, is created to read: <u>20.70 Agency for State Systems and Enterprise Technology</u> <u>There is created the Agency for State Systems and Enterprise</u> <u>Technology. The head of the agency is the Governor and Cabinet.</u> <u>(1) DIVISIONS AND OFFICESThe following divisions and</u> <u>offices of the Agency for State Systems and Enterprise</u> <u>Technology are established:</u> <u>(a) The Division of Administrative Services.</u> 	335	providing effective dates.
338 339 Section 1. Section 20.70, Florida Statutes, is created to 340 read: 341 <u>20.70 Agency for State Systems and Enterprise Technology</u> 342 <u>There is created the Agency for State Systems and Enterprise</u> 343 <u>Technology. The head of the agency is the Governor and Cabinet.</u> 344 <u>(1) DIVISIONS AND OFFICESThe following divisions and 345 offices of the Agency for State Systems and Enterprise</u> 346 <u>Technology are established:</u> 347 <u>(a) The Division of Administrative Services.</u>	336	
Section 1. Section 20.70, Florida Statutes, is created to read: 20.70 Agency for State Systems and Enterprise Technology.— There is created the Agency for State Systems and Enterprise Technology. The head of the agency is the Governor and Cabinet. (1) DIVISIONS AND OFFICES.—The following divisions and offices of the Agency for State Systems and Enterprise Technology are established: (a) The Division of Administrative Services.	337	Be It Enacted by the Legislature of the State of Florida:
<pre>340 341 341 341 <u>20.70 Agency for State Systems and Enterprise Technology</u> 342 342 <u>There is created the Agency for State Systems and Enterprise</u> 343 <u>Technology. The head of the agency is the Governor and Cabinet.</u> 344 <u>(1) DIVISIONS AND OFFICESThe following divisions and</u> 345 <u>offices of the Agency for State Systems and Enterprise</u> 346 <u>Technology are established:</u> 347 <u>(a) The Division of Administrative Services.</u></pre>	338	
 341 <u>20.70 Agency for State Systems and Enterprise Technology</u> 342 <u>There is created the Agency for State Systems and Enterprise</u> 343 <u>Technology. The head of the agency is the Governor and Cabinet.</u> 344 <u>(1) DIVISIONS AND OFFICESThe following divisions and</u> 345 <u>offices of the Agency for State Systems and Enterprise</u> 346 <u>Technology are established:</u> 347 <u>(a) The Division of Administrative Services.</u> 	339	Section 1. Section 20.70, Florida Statutes, is created to
342There is created the Agency for State Systems and Enterprise343Technology. The head of the agency is the Governor and Cabinet.344(1) DIVISIONS AND OFFICES.—The following divisions and345offices of the Agency for State Systems and Enterprise346Technology are established:347(a) The Division of Administrative Services.	340	read:
343Technology. The head of the agency is the Governor and Cabinet.344(1) DIVISIONS AND OFFICES.—The following divisions and345offices of the Agency for State Systems and Enterprise346Technology are established:347(a) The Division of Administrative Services.		
 344 (1) DIVISIONS AND OFFICES.—The following divisions and 345 offices of the Agency for State Systems and Enterprise 346 Technology are established: 347 (a) The Division of Administrative Services. 		
345 <u>offices of the Agency for State Systems and Enterprise</u> 346 <u>Technology are established:</u> 347 <u>(a) The Division of Administrative Services.</u>		Technology. The head of the agency is the Governor and Cabinet.
346 <u>Technology are established:</u> 347 <u>(a) The Division of Administrative Services.</u>		
347 (a) The Division of Administrative Services.		
348 (b) The Office of Information Technology.		
	348	(b) The Office of Information Technology.

Page 12 of 111

	576-02644-25 20257026
349	(c) Beginning July 1, 2026:
350	1. The Division of Enterprise Data and Interoperability.
351	2. The Division of Enterprise Security.
352	3. The Division of Enterprise Information Technology
353	Services.
354	4. The Division of Enterprise Information Technology
355	Purchasing.
356	5. The Division of Enterprise Information Technology
357	Workforce Development.
358	(2) EXECUTIVE DIRECTORThe executive director of the
359	Agency for State Systems and Enterprise Technology also serves
360	as the state chief information officer. The Governor and Cabinet
361	shall appoint a state chief information officer from nominees of
362	the state chief information officer selection committee. The
363	appointment must be made by a majority vote of the Governor and
364	Cabinet and is subject to confirmation by the Senate. Removal of
365	the state chief information officer is subject to a majority
366	vote of the Governor and Cabinet. The state chief information
367	officer is prohibited from having any financial, personal, or
368	business conflicts of interest related to technology vendors,
369	contractors, or other information technology service providers
370	doing business with the state.
371	(3) STATE CHIEF INFORMATION OFFICER SELECTION COMMITTEE
372	(a) Upon a vacancy or anticipated vacancy, the state chief
373	information officer selection committee within the Agency for
374	State Systems and Enterprise Technology shall be appointed to
375	nominate up to three qualified appointees for the position of
376	state chief information officer to the Governor and Cabinet for
377	appointment.

Page 13 of 111

	576-02644-25 20257026
378	(b) The selection committee shall be composed of the
379	following members:
380	1. A state agency chief information officer of an executive
381	agency, appointed by the Governor and who shall serve as chair
382	of the committee.
383	2. The chief information officer of the Department of
384	Agriculture and Consumer Services, appointed by the Commissioner
385	of Agriculture.
386	3. The chief information officer of the Department of
387	Financial Services, appointed by the Chief Financial Officer.
388	4. The chief information officer of the Department of Legal
389	Affairs, appointed by the Attorney General.
390	(c) If a member of the selection committee submits an
391	application to be considered for the position of state chief
392	information officer, the member must designate an alternate
393	state agency chief information officer to serve on the
394	committee.
395	(4) QUALIFICATIONS FOR THE STATE CHIEF INFORMATION
396	OFFICER
397	(a) Education requirementsThe state chief information
398	officer must meet one of the following criteria:
399	1. Hold a bachelor's degree from an accredited institution
400	in information technology, computer science, business
401	administration, public administration, or a related field; or
402	2. Hold a master's degree in any of the fields listed
403	above, which may be substituted for a portion of the experience
404	requirement, as determined by the selection committee.
405	(b) Professional experience requirementsThe state chief
406	information officer must have at least 10 years of progressively

Page 14 of 111

407 <u>responsible experience in information te</u> 408 digital transformation, cybersecurity, c	
408 digital transformation, cybersecurity, c	or information technology
409 governance, including:	
410 <u>1. A minimum of 5 years in an exec</u>	utive or senior
411 leadership role, overseeing information	technology strategy,
412 operations, or enterprise technology man	nagement in either the
413 <u>public or private sector;</u>	
414 <u>2. Managing large-scale information</u>	on technology projects,
415 enterprise infrastructure, and implement	tation of emerging
416 technologies;	
417 <u>3. Budget planning, procurement ov</u>	versight, and financial
418 management of information technology inv	vestments; and
419 <u>4. Working with state and federal</u>	information technology
420 regulations, digital services, and cyber	rsecurity compliance
421 <u>frameworks.</u>	
422 (c) Technical and policy expertise	eThe state chief
423 information officer must have demonstrat	ted expertise in:
424 <u>1. Cybersecurity and data protecti</u>	on by demonstrating
425 knowledge of cybersecurity risk manageme	ent, compliance with
426 NIST, ISO 27001, and applicable federal	and state security
427 regulations;	
428 <u>2. Cloud and digital services with</u>	experience with cloud
429 computing, enterprise systems modernizat	tion, digital
430 transformation, and emerging information	n technology trends;
431 <u>3. Information technology governan</u>	ice and policy development
432 by demonstrating an understanding of sta	atewide information
433 technology governance structures, digita	al services, and
434 information technology procurement polic	cies; and
435 <u>4. Public sector information techn</u>	ology management by

Page 15 of 111

 demonstrating familiarity with government information technology funding models, procurement requirements, and legislative processes affecting information technology strategy. (d) Leadership and administrative competencies.—The state chief information officer must demonstrate: Strategic vision and innovation by possessing the capability to modernize information technology systems, drive digital transformation, and align information technology initiatives with state goals; Collaboration and engagement with stakeholders by working with legislators, state agency heads, local governments, and private sector partners to implement information technology initiatives; Scrisis management and cyber resilience by possessing the capability to develop and lead cyber incident response, disaster recovery, and information technology budgets, cost-control strategies, and financial oversight of information technology projects. (e) Previous appointment or service.—A person who is currently serving or has previously served as the head of a state agency in the state is ineligible for nomination, appointment, or service as the state chief information officer. Section 2. Until a state chief information officer is 		576-02644-25 20257026
438processes affecting information technology strategy.439(d) Leadership and administrative competencies.—The state440chief information officer must demonstrate:4411. Strategic vision and innovation by possessing the442capability to modernize information technology systems, drive443digital transformation, and align information technology444initiatives with state goals;4452. Collaboration and engagement with stakeholders by446working with legislators, state agency heads, local governments,447and private sector partners to implement information technology448initiatives;4493. Crisis management and cyber resilience by possessing the450capability to develop and lead cyber incident response, disaster451recovery, and information technology budgets, cost-control4524. Fiscal management and budget expertise managing multi-453million-dollar information technology budgets, cost-control454strategies, and financial oversight of information technology455projects.456(e) Previous appointment or serviceA person who is457currently serving or has previously served as the head of a458state agency in the state is ineligible for nomination,459appointment, or service as the state chief information officer.460Section 2. Until a state chief information officer is	436	demonstrating familiarity with government information technology
439(d) Leadership and administrative competenciesThe state440chief information officer must demonstrate:4411. Strategic vision and innovation by possessing the442capability to modernize information technology systems, drive443digital transformation, and align information technology444initiatives with state goals;4452. Collaboration and engagement with stakeholders by446working with legislators, state agency heads, local governments,447and private sector partners to implement information technology448initiatives;4493. Crisis management and cyber resilience by possessing the450capability to develop and lead cyber incident response, disaster451recovery, and information technology continuity plans; and4524. Fiscal management and budget expertise managing multi-453million-dollar information technology budgets, cost-control454strategies, and financial oversight of information technology455projects.456(e) Previous appointment or serviceA person who is457currently serving or has previously served as the head of a458state agency in the state is ineligible for nomination,459appointment, or service as the state chief information officer.460Section 2. Until a state chief information officer is	437	funding models, procurement requirements, and legislative
 chief information officer must demonstrate: Strategic vision and innovation by possessing the capability to modernize information technology systems, drive digital transformation, and align information technology initiatives with state goals; 2. Collaboration and engagement with stakeholders by working with legislators, state agency heads, local governments, and private sector partners to implement information technology initiatives; 3. Crisis management and cyber resilience by possessing the capability to develop and lead cyber incident response, disaster recovery, and information technology budgets, cost-control strategies, and financial oversight of information technology projects. (e) Previous appointment or serviceA person who is currently serving or has previously served as the head of a state agency in the state is ineligible for nomination, appointment, or service as the state chief information officer. 	438	processes affecting information technology strategy.
 1. Strategic vision and innovation by possessing the capability to modernize information technology systems, drive digital transformation, and align information technology initiatives with state goals; 2. Collaboration and engagement with stakeholders by working with legislators, state agency heads, local governments, and private sector partners to implement information technology initiatives; 3. Crisis management and cyber resilience by possessing the capability to develop and lead cyber incident response, disaster recovery, and information technology budgets, cost-control strategies, and financial oversight of information technology projects. (e) Previous appointment or serviceA person who is currently serving or has previously served as the head of a state agency in the state is ineligible for nomination, appointment, or service as the state chief information officer. Section 2. Until a state chief information officer is 	439	(d) Leadership and administrative competenciesThe state
442 capability to modernize information technology systems, drive 443 digital transformation, and align information technology 444 initiatives with state goals; 445 2. Collaboration and engagement with stakeholders by 446 working with legislators, state agency heads, local governments, 447 and private sector partners to implement information technology 448 initiatives; 449 3. Crisis management and cyber resilience by possessing the 450 capability to develop and lead cyber incident response, disaster 451 recovery, and information technology continuity plans; and 452 4. Fiscal management and budget expertise managing multi- 453 million-dollar information technology budgets, cost-control 454 strategies, and financial oversight of information technology 455 projects. 456 (e) Previous appointment or serviceA person who is 457 currently serving or has previously served as the head of a 458 state agency in the state is ineligible for nomination, 459 appointment, or service as the state chief information officer. 460 Section 2. Until a state chief information officer is	440	chief information officer must demonstrate:
 digital transformation, and align information technology initiatives with state goals; 2. Collaboration and engagement with stakeholders by working with legislators, state agency heads, local governments, and private sector partners to implement information technology initiatives; 3. Crisis management and cyber resilience by possessing the capability to develop and lead cyber incident response, disaster recovery, and information technology continuity plans; and 4. Fiscal management and budget expertise managing multi- million-dollar information technology budgets, cost-control strategies, and financial oversight of information technology projects. (e) Previous appointment or serviceA person who is currently serving or has previously served as the head of a state agency in the state is ineligible for nomination, appointment, or service as the state chief information officer. Section 2. Until a state chief information officer is 	441	1. Strategic vision and innovation by possessing the
 initiatives with state goals; 2. Collaboration and engagement with stakeholders by working with legislators, state agency heads, local governments, and private sector partners to implement information technology initiatives; 3. Crisis management and cyber resilience by possessing the capability to develop and lead cyber incident response, disaster recovery, and information technology continuity plans; and 4. Fiscal management and budget expertise managing multi- million-dollar information technology budgets, cost-control strategies, and financial oversight of information technology projects. (e) Previous appointment or serviceA person who is currently serving or has previously served as the head of a state agency in the state is ineligible for nomination, appointment, or service as the state chief information officer. Section 2. Until a state chief information officer is 	442	capability to modernize information technology systems, drive
 2. Collaboration and engagement with stakeholders by working with legislators, state agency heads, local governments, and private sector partners to implement information technology initiatives; 3. Crisis management and cyber resilience by possessing the capability to develop and lead cyber incident response, disaster recovery, and information technology continuity plans; and 4. Fiscal management and budget expertise managing multi- million-dollar information technology budgets, cost-control strategies, and financial oversight of information technology projects. (e) Previous appointment or serviceA person who is currently serving or has previously served as the head of a state agency in the state is ineligible for nomination, appointment, or service as the state chief information officer. Section 2. Until a state chief information officer is 	443	digital transformation, and align information technology
446 working with legislators, state agency heads, local governments, 447 and private sector partners to implement information technology 448 initiatives; 449 3. Crisis management and cyber resilience by possessing the 450 capability to develop and lead cyber incident response, disaster 451 recovery, and information technology continuity plans; and 452 4. Fiscal management and budget expertise managing multi- 453 million-dollar information technology budgets, cost-control 454 strategies, and financial oversight of information technology 455 projects. 456 (e) Previous appointment or serviceA person who is 457 currently serving or has previously served as the head of a 458 state agency in the state is ineligible for nomination, 459 appointment, or service as the state chief information officer. 460 Section 2. Until a state chief information officer is	444	initiatives with state goals;
447 and private sector partners to implement information technology 448 initiatives; 449 3. Crisis management and cyber resilience by possessing the capability to develop and lead cyber incident response, disaster 450 450 450 451 452 453 454 455 455 455 455 (e) Previous appointment or serviceA person who is 455 456 (e) Previous appointment or serviceA person who is 457 458 456 456 457 456 457 458 457 458 457 458 458 458 459 459 459 459 459 459 459 459 459 459	445	2. Collaboration and engagement with stakeholders by
initiatives; 3. Crisis management and cyber resilience by possessing the capability to develop and lead cyber incident response, disaster recovery, and information technology continuity plans; and 4. Fiscal management and budget expertise managing multi- million-dollar information technology budgets, cost-control strategies, and financial oversight of information technology projects. (e) Previous appointment or service.—A person who is currently serving or has previously served as the head of a state agency in the state is ineligible for nomination, appointment, or service as the state chief information officer. Section 2. Until a state chief information officer is	446	working with legislators, state agency heads, local governments,
 3. Crisis management and cyber resilience by possessing the capability to develop and lead cyber incident response, disaster recovery, and information technology continuity plans; and 4. Fiscal management and budget expertise managing multi- million-dollar information technology budgets, cost-control strategies, and financial oversight of information technology projects. (e) Previous appointment or serviceA person who is currently serving or has previously served as the head of a state agency in the state is ineligible for nomination, appointment, or service as the state chief information officer. Section 2. Until a state chief information officer is 	447	and private sector partners to implement information technology
450 <u>capability to develop and lead cyber incident response, disaster</u> 451 <u>recovery, and information technology continuity plans; and</u> 452 <u>4. Fiscal management and budget expertise managing multi-</u> 453 <u>million-dollar information technology budgets, cost-control</u> 454 <u>strategies, and financial oversight of information technology</u> 455 <u>projects.</u> 456 <u>(e) Previous appointment or serviceA person who is</u> 457 <u>currently serving or has previously served as the head of a</u> 458 <u>state agency in the state is ineligible for nomination,</u> 459 <u>appointment, or service as the state chief information officer.</u> 460 <u>Section 2. Until a state chief information officer is</u>	448	initiatives;
451 recovery, and information technology continuity plans; and 452 <u>4. Fiscal management and budget expertise managing multi-</u> 453 million-dollar information technology budgets, cost-control 454 strategies, and financial oversight of information technology 455 projects. 456 <u>(e) Previous appointment or serviceA person who is</u> 457 currently serving or has previously served as the head of a 458 state agency in the state is ineligible for nomination, 459 appointment, or service as the state chief information officer. 460 Section 2. Until a state chief information officer is	449	3. Crisis management and cyber resilience by possessing the
 452 4. Fiscal management and budget expertise managing multi- 453 million-dollar information technology budgets, cost-control 454 455 strategies, and financial oversight of information technology 455 projects. 456 (e) Previous appointment or serviceA person who is 457 currently serving or has previously served as the head of a 458 state agency in the state is ineligible for nomination, 459 appointment, or service as the state chief information officer. 460 Section 2. Until a state chief information officer is 	450	capability to develop and lead cyber incident response, disaster
 453 million-dollar information technology budgets, cost-control 454 strategies, and financial oversight of information technology 455 projects. 456 (e) Previous appointment or serviceA person who is 457 currently serving or has previously served as the head of a 458 state agency in the state is ineligible for nomination, 459 appointment, or service as the state chief information officer. 460 Section 2. Until a state chief information officer is 	451	recovery, and information technology continuity plans; and
 454 strategies, and financial oversight of information technology 455 projects. 456 (e) Previous appointment or service.—A person who is 457 currently serving or has previously served as the head of a 458 state agency in the state is ineligible for nomination, 459 appointment, or service as the state chief information officer. 460 Section 2. Until a state chief information officer is 	452	4. Fiscal management and budget expertise managing multi-
 455 projects. 456 (e) Previous appointment or service.—A person who is 457 currently serving or has previously served as the head of a 458 state agency in the state is ineligible for nomination, 459 appointment, or service as the state chief information officer. 460 Section 2. Until a state chief information officer is 	453	million-dollar information technology budgets, cost-control
 456 (e) Previous appointment or service.—A person who is 457 currently serving or has previously served as the head of a 458 state agency in the state is ineligible for nomination, 459 appointment, or service as the state chief information officer. 460 Section 2. Until a state chief information officer is 	454	strategies, and financial oversight of information technology
 457 <u>currently serving or has previously served as the head of a</u> 458 <u>state agency in the state is ineligible for nomination,</u> 459 <u>appointment, or service as the state chief information officer.</u> 460 Section 2. <u>Until a state chief information officer is</u> 	455	projects.
 458 state agency in the state is ineligible for nomination, 459 appointment, or service as the state chief information officer. 460 Section 2. Until a state chief information officer is 	456	(e) Previous appointment or serviceA person who is
459 <u>appointment</u> , or service as the state chief information officer. 460 Section 2. <u>Until a state chief information officer is</u>	457	currently serving or has previously served as the head of a
460 Section 2. <u>Until a state chief information officer is</u>	458	state agency in the state is ineligible for nomination,
	459	appointment, or service as the state chief information officer.
461 <u>appointed pursuant to s. 20.70, Florida Statutes, the current</u>	460	Section 2. Until a state chief information officer is
	461	appointed pursuant to s. 20.70, Florida Statutes, the current
462 state chief information officer of the Department of Management	462	state chief information officer of the Department of Management
463 <u>Services shall be transferred to the Agency for State Systems</u>	463	Services shall be transferred to the Agency for State Systems
464 and Enterprise Technology and serve as interim state chief	464	and Enterprise Technology and serve as interim state chief

Page 16 of 111

	576-02644-25 20257026
465	information officer. A state chief information officer for the
466	Agency for State Systems and Enterprise Technology must be
467	appointed by the Governor and Cabinet by January 2, 2026.
468	Appointments to the state chief information officer selection
469	committee must be made by August 1, 2025.
470	Section 3. Effective July 1, 2026, paragraph (b) of
471	subsection (3) of section 97.0525, Florida Statutes, is amended
472	to read:
473	97.0525 Online voter registration
474	(3)
475	(b) The division shall conduct a comprehensive risk
476	assessment of the online voter registration system every 2
477	years. The comprehensive risk assessment must comply with the
478	risk assessment methodology developed by the <u>Agency for State</u>
479	Systems and Enterprise Technology Department of Management
480	Services for identifying security risks, determining the
481	magnitude of such risks, and identifying areas that require
482	safeguards. In addition, the comprehensive risk assessment must
483	incorporate all of the following:
484	1. Load testing and stress testing to ensure that the
485	online voter registration system has sufficient capacity to
486	accommodate foreseeable use, including during periods of high
487	volume of website users in the week immediately preceding the
488	book-closing deadline for an election.
489	2. Screening of computers and networks used to support the
490	online voter registration system for malware and other
491	vulnerabilities.
492	3. Evaluation of database infrastructure, including
493	software and operating systems, in order to fortify defenses
	Page 17 of 111

	576-02644-25 20257026
494	against cyberattacks.
495	4. Identification of any anticipated threats to the
496	security and integrity of data collected, maintained, received,
497	or transmitted by the online voter registration system.
498	Section 4. Effective July 1, 2026, paragraphs (a) and (f)
499	of subsection (1), paragraphs (b) and (c) of subsection (2), and
500	subsections (3) and (4) of section 112.22, Florida Statutes, are
501	amended to read:
502	112.22 Use of applications from foreign countries of
503	concern prohibited
504	(1) As used in this section, the term:
505	(a) "ASSET" means the Agency for State Systems and
506	Enterprise Technology "Department" means the Department of
507	Management Services.
508	(f) "Prohibited application" means an application that
509	meets the following criteria:
510	1. Any Internet application that is created, maintained, or
511	owned by a foreign principal and that participates in activities
512	that include, but are not limited to:
513	a. Collecting keystrokes or sensitive personal, financial,
514	proprietary, or other business data;
515	b. Compromising e-mail and acting as a vector for
516	ransomware deployment;
517	c. Conducting cyber-espionage against a public employer;
518	d. Conducting surveillance and tracking of individual
519	users; or
520	e. Using algorithmic modifications to conduct
521	disinformation or misinformation campaigns; or
522	2. Any Internet application <u>ASSET</u> the department deems to
	Page 18 of 111

	576-02644-25 20257026
523	present a security risk in the form of unauthorized access to or
524	temporary unavailability of the public employer's records,
525	digital assets, systems, networks, servers, or information.
526	(2)
527	(b) A person, including an employee or officer of a public
528	employer, may not download or access any prohibited application
529	on any government-issued device.
530	1. This paragraph does not apply to a law enforcement
531	officer as defined in s. 943.10(1) if the use of the prohibited
532	application is necessary to protect the public safety or conduct
533	an investigation within the scope of his or her employment.
534	2. A public employer may request a waiver from <u>ASSET</u> the
535	department to allow designated employees or officers to download
536	or access a prohibited application on a government-issued
537	device.
538	(c) Within 15 calendar days after <u>ASSET</u> the department
539	issues or updates its list of prohibited applications pursuant
540	to paragraph (3)(a), an employee or officer of a public employer
541	who uses a government-issued device must remove, delete, or
542	uninstall any prohibited applications from his or her
543	government-issued device.
544	(3) ASSET The department shall do all of the following:
545	(a) Compile and maintain a list of prohibited applications
546	and publish the list on its website. $\underline{ ext{ASSET}}$ $\overline{ ext{The department}}$ shall
547	update this list quarterly and shall provide notice of any
548	update to public employers.
549	(b) Establish procedures for granting or denying requests
550	for waivers pursuant to subparagraph (2)(b)2. The request for a
551	waiver must include all of the following:
I	Page 19 of 111

	576-02644-25 20257026
552	1. A description of the activity to be conducted and the
553	state interest furthered by the activity.
554	2. The maximum number of government-issued devices and
555	employees or officers to which the waiver will apply.
556	3. The length of time necessary for the waiver. Any waiver
557	granted pursuant to subparagraph (2)(b)2. must be limited to a
558	timeframe of no more than 1 year, but <u>ASSET</u> the department may
559	approve an extension.
560	4. Risk mitigation actions that will be taken to prevent
561	access to sensitive data, including methods to ensure that the
562	activity does not connect to a state system, network, or server.
563	5. A description of the circumstances under which the
564	waiver applies.
565	(4) (a) Notwithstanding s. 120.74(4) and (5), the department
566	is authorized, and all conditions are deemed met, to adopt
567	emergency rules pursuant to s. 120.54(4) and to implement
568	paragraph (3)(a). Such rulemaking must occur initially by filing
569	emergency rules within 30 days after July 1, 2023.
570	(b) ASSET The department shall adopt rules necessary to
571	administer this section.
572	Section 5. Effective July 1, 2026, paragraph (a) of
573	subsection (5) of section 119.0725, Florida Statutes, is amended
574	to read:
575	119.0725 Agency cybersecurity information; public records
576	exemption; public meetings exemption
577	(5)(a) Information made confidential and exempt pursuant to
578	this section <u>must</u> shall be made available to a law enforcement
579	agency, the Auditor General, the Cybercrime Office of the
580	Department of Law Enforcement, the <u>Agency for State Systems and</u>

Page 20 of 111

	576-02644-25 20257026
581	Enterprise Technology Florida Digital Service within the
582	Department of Management Services, and, for agencies under the
583	jurisdiction of the Governor, the Chief Inspector General.
584	Section 6. Subsection (7) of section 216.023, Florida
585	Statutes, is amended to read:
586	216.023 Legislative budget requests to be furnished to
587	Legislature by agencies
588	(7) As part of the legislative budget request, each state
589	agency and the judicial branch shall include <u>a cumulative</u> an
590	inventory <u>and status report</u> of all ongoing technology-related
591	projects ongoing during the prior fiscal year or undertaken in
592	the prior fiscal year. For the purposes of this subsection, the
593	term "technology-related project" means a project that has been
594	funded or has had or is expected to have expenditures in more
595	than one fiscal year; has that have a cumulative estimated or
596	realized cost of more than \$1 million; and does not include the
597	continuance of existing hardware and software maintenance
598	agreements, renewal of existing software licensing agreements,
599	or the replacement of desktop units with new technology that is
600	substantially similar to the technology being replaced. The
601	inventory must, at a minimum, contain all of the following
602	information:
603	(a) The name of the technology system.
604	(b) A brief description of the purpose and function of the
605	system.
606	(c) A brief description of the goals of the project.
607	(d) The initiation date of the project.
608	(e) The key performance indicators for the project.
609	(f) Any other metrics for the project evaluating the health
	Page 21 of 111

	576-02644-25 20257026
610	and status of the project.
611	(g) The original and current baseline estimated end dates
612	of the project.
613	(h) The original and current estimated costs of the
614	project.
615	(i) Total funds appropriated or allocated to the project
616	and the current realized cost for the project by fiscal year.
617	
618	For purposes of this subsection, an ongoing technology-related
619	project is one which has been funded or has had or is expected
620	to have expenditures in more than one fiscal year. An ongoing
621	technology-related project does not include the continuance of
622	existing hardware and software maintenance agreements, the
623	renewal of existing software licensing agreements, or the
624	replacement of desktop units with new technology that is
625	substantially similar to the technology being replaced. This
626	subsection expires July 1, 2025.
627	Section 7. Effective July 1, 2026, paragraph (a) of
628	subsection (4) and subsection (7) of section 216.023, Florida
629	Statutes, are amended to read:
630	216.023 Legislative budget requests to be furnished to
631	Legislature by agencies
632	(4)(a) The legislative budget request for each program must
633	contain:
634	1. The constitutional or statutory authority for a program,
635	a brief purpose statement, and approved program components.
636	2. Information on expenditures for 3 fiscal years (actual
637	prior-year expenditures, current-year estimated expenditures,
638	and agency budget requested expenditures for the next fiscal
	Page 22 of 111

576-02644-25 20257026 639 year) by appropriation category. 640 3. Details on trust funds and fees. 641 The total number of positions (authorized, fixed, and 4. 642 requested). 643 5. An issue narrative describing and justifying changes in 644 amounts and positions requested for current and proposed 645 programs for the next fiscal year. 646 6. Information resource requests. 647 Supporting information, including applicable cost-7. 648 benefit analyses, business case analyses, performance 649 contracting procedures, service comparisons, and impacts on 650 performance standards for any request to outsource or privatize 651 state agency functions. The cost-benefit and business case 652 analyses must include an assessment of the impact on each 653 affected activity from those identified in accordance with 654 paragraph (b). Performance standards must include standards for 655 each affected activity and be expressed in terms of the 656 associated unit of activity. 657 8. An evaluation of major outsourcing and privatization 658 initiatives undertaken during the last 5 fiscal years having 659 aggregate expenditures exceeding \$10 million during the term of 660 the contract. The evaluation must include an assessment of contractor performance, a comparison of anticipated service 661 662 levels to actual service levels, and a comparison of estimated 663 savings to actual savings achieved. Consolidated reports issued 664 by the Department of Management Services may be used to satisfy

666 9. Supporting information for any proposed consolidated667 financing of deferred-payment commodity contracts including

665

this requirement.

Page 23 of 111

CODING: Words stricken are deletions; words underlined are additions.

576-02644-25 20257026 668 quaranteed energy performance savings contracts. Supporting 669 information must also include narrative describing and 670 justifying the need, baseline for current costs, estimated cost 671 savings, projected equipment purchases, estimated contract 672 costs, and return on investment calculation. 673 10. For projects that exceed \$10 million in total cost, the 674 statutory reference of the existing policy or the proposed 675 substantive policy that establishes and defines the project's 676 governance structure, planned scope, main business objectives 677 that must be achieved, and estimated completion timeframes. The 678 governance structure for information technology-related projects 679 must incorporate the applicable project management and oversight 680 standards established pursuant to s. 282.0061 s. 282.0051. Information technology budget requests for the continuance of 681 existing hardware and software maintenance agreements, renewal 682 683 of existing software licensing agreements, or the replacement of desktop units with new technology that is similar to the 684 685 technology currently in use are exempt from this requirement. 686 (7) As part of the legislative budget request, each state 687 agency and the judicial branch shall include a cumulative 688 inventory and status report of all technology-related projects 689 ongoing during the prior fiscal year or undertaken in the prior 690 fiscal year. For the purposes of this subsection, the term "technology-related project" means a project that has been 691 692 funded or has had or is expected to have expenditures in more 693 than one fiscal year; has a cumulative estimated or realized 694 cost of more than \$1 million; and does not include the 695 continuance of existing hardware and software maintenance 696 agreements, renewal of existing software licensing agreements,

Page 24 of 111

CODING: Words stricken are deletions; words underlined are additions.

	576-02644-25 20257026
697	or the replacement of desktop units with new technology that is
698	substantially similar to the technology being replaced. The
699	inventory must, at a minimum, contain all of the following
700	information:
701	(a) The name of the technology system.
702	(b) A brief description of the purpose and function of the
703	system.
704	(c) A brief description of the goals of the project.
705	(d) The initiation date of the project.
706	(e) The key performance indicators for the project.
707	(f) Any other metrics for the project evaluating the health
708	and status of the project.
709	(g) The original and current baseline estimated end dates
710	of the project.
711	(h) The original and current estimated costs of the
712	project.
713	(i) — Total funds appropriated or allocated to the project
714	and the current realized cost for the project by fiscal year.
715	Section 8. Present subsections (36), (37), and (38) of
716	section 282.0041, Florida Statutes, are redesignated as
717	subsections (37), (38), and (39), respectively, and a new
718	subsection (36) is added to that section, and subsections (1)
719	and (34) of that section are amended, to read:
720	282.0041 DefinitionsAs used in this chapter, the term:
721	(1) "ASSET" means the Agency for State Systems and
722	Enterprise Technology
723	customer entity must pay annually for services from the
724	Department of Management Services and includes administrative
725	and data center services costs.

Page 25 of 111

1	576-02644-25 20257026
726	(34) "State agency" means any official, officer,
727	commission, board, authority, council, committee, or department
728	of the executive branch of state government; the Justice
729	Administrative Commission; and the Public Service Commission.
730	The term does not include university boards of trustees or state
731	universities. As used in part I of this chapter, except as
732	otherwise specifically provided, the term <u>includes does not</u>
733	include the Department of Legal Affairs, the Department of
734	Agriculture and Consumer Services, <u>and</u> or the Department of
735	Financial Services.
736	(36) "Technical debt" means the accumulated cost and
737	operational impact resulting from the use of suboptimal,
738	expedient, or outdated technology solutions that require future
739	remediation, refactoring, or replacement to ensure
740	maintainability, security, efficiency, and compliance with
741	enterprise architecture standards.
742	Section 9. Section 282.0051, Florida Statutes, is amended
743	to read:
744	282.0051 Department of Management Services; Florida Digital
745	Service; powers, duties, and functions
746	(1) The Florida Digital Service has been created within the
747	department to propose innovative solutions that securely
748	modernize state government, including technology and information
749	services, to achieve value through digital transformation and
750	interoperability, and to fully support the cloud-first policy as
751	specified in s. 282.206. The department, through the Florida
752	Digital Service, shall have the following powers, duties, and
753	functions:
754	(a) Assign and document state agency technical debt and
I	

Page 26 of 111

	576-02644-25 20257026
755	security risks. All results of the assessments and all
756	documentation, including source documents, meeting notes, and
757	internal work products, must be provided in native electronic
758	and paper formats to ASSET no later than June 15, 2026.
759	(b) Facilitate the transfer of existing cybersecurity tools
760	and services, provided to state agencies by the department
761	through the Florida Digital Service, directly to the respective
762	state agencies, accompanied by the necessary training, no later
763	than September 15, 2025.
764	(c) Direct the state chief information security officer to
765	provide a consolidated cybersecurity incident report by the 30th
766	day after the end of each quarter to the interim state chief
767	information officer, the Executive Office of the Governor, the
768	Commissioner of Agriculture, the Chief Financial Officer, the
769	Attorney General, the President of the Senate, and the Speaker
770	of the House of Representatives Develop and publish information
771	technology policy for the management of the state's information
772	technology resources.
773	(b) Develop an enterprise architecture that:
774	1. Acknowledges the unique needs of the entities within the
775	enterprise in the development and publication of standards and
776	terminologies to facilitate digital interoperability;
777	2.—Supports the cloud-first policy as specified in s.
778	282.206; and
779	3. Addresses how information technology infrastructure may
780	be modernized to achieve cloud-first objectives.
781	(c) Establish project management and oversight standards
782	with which state agencies must comply when implementing
783	information technology projects. The department, acting through
I	Page 27 of 111

Page 27 of 111

	576-02644-25 20257026
784	the Florida Digital Service, shall provide training
785	opportunities to state agencies to assist in the adoption of the
786	project management and oversight standards. To support data-
787	driven decisionmaking, the standards must include, but are not
788	limited to:
789	1. Performance measurements and metrics that objectively
790	reflect the status of an information technology project based on
791	a defined and documented project scope, cost, and schedule.
792	2. Methodologies for calculating acceptable variances in
793	the projected versus actual scope, schedule, or cost of an
794	information technology project.
795	3. Reporting requirements, including requirements designed
796	to alert all defined stakeholders that an information technology
797	project has exceeded acceptable variances defined and documented
798	in a project plan.
799	4. Content, format, and frequency of project updates.
800	5. Technical standards to ensure an information technology
801	project complies with the enterprise architecture.
802	(d) Perform project oversight on all state agency
803	information technology projects that have total project costs of
804	\$10 million or more and that are funded in the General
805	Appropriations Act or any other law. The department, acting
806	through the Florida Digital Service, shall report at least
807	quarterly to the Executive Office of the Governor, the President
808	of the Senate, and the Speaker of the House of Representatives
809	on any information technology project that the department
810	identifies as high-risk due to the project exceeding acceptable
811	variance ranges defined and documented in a project plan. The
812	report must include a risk assessment, including fiscal risks,

Page 28 of 111

	576-02644-25 20257026
813	associated with proceeding to the next stage of the project, and
814	a recommendation for corrective actions required, including
815	suspension or termination of the project.
816	(c) Identify opportunities for standardization and
817	consolidation of information technology services that support
818	interoperability and the cloud-first policy, as specified in s.
819	282.206, and business functions and operations, including
820	administrative functions such as purchasing, accounting and
821	reporting, cash management, and personnel, and that are common
822	across state agencies. The department, acting through the
823	Florida Digital Service, shall biennially on January 1 of each
824	even-numbered year provide recommendations for standardization
825	and consolidation to the Executive Office of the Governor, the
826	President of the Senate, and the Speaker of the House of
827	Representatives.
828	(f) Establish best practices for the procurement of
829	information technology products and cloud-computing services in
830	order to reduce costs, increase the quality of data center
831	services, or improve government services.
832	(g) — Develop standards for information technology reports
833	and updates, including, but not limited to, operational work
834	plans, project spend plans, and project status reports, for use
835	by state agencies.
836	(h) Upon request, assist state agencies in the development
837	of information technology-related legislative budget requests.
838	(i) Conduct annual assessments of state agencies to
839	determine compliance with all information technology standards
840	and guidelines developed and published by the department and
841	provide results of the assessments to the Executive Office of

Page 29 of 111

576-02644-25 20257026 842 the Governor, the President of the Senate, and the Speaker of 843 the House of Representatives. 844 (j) Conduct a market analysis not less frequently than 845 every 3 years beginning in 2021 to determine whether the 846 information technology resources within the enterprise are 847 utilized in the most cost-effective and cost-efficient manner, 848 while recognizing that the replacement of certain legacy 849 information technology systems within the enterprise may be cost 850 prohibitive or cost inefficient due to the remaining useful life of those resources; whether the enterprise is complying with the 851 852 cloud-first policy specified in s. 282.206; and whether the 853 enterprise is utilizing best practices with respect to 854 information technology, information services, and the 855 acquisition of emerging technologies and information services. 856 Each market analysis shall be used to prepare a strategic plan 857 for continued and future information technology and information 858 services for the enterprise, including, but not limited to, 859 proposed acquisition of new services or technologies and 860 approaches to the implementation of any new services or 861 technologies. Copies of each market analysis and accompanying 862 strategic plan must be submitted to the Executive Office of the 863 Governor, the President of the Senate, and the Speaker of the 864 House of Representatives not later than December 31 of each year that a market analysis is conducted. 865 866 (k) Recommend other information technology services that 867 should be designed, delivered, and managed as enterprise 868 information technology services. Recommendations must include 869 the identification of existing information technology resources 870 associated with the services, if existing services must be

Page 30 of 111

	576-02644-25 20257026
871	transferred as a result of being delivered and managed as
872	enterprise information technology services.
873	(1) In consultation with state agencies, propose a
874	methodology and approach for identifying and collecting both
875	current and planned information technology expenditure data at
876	the state agency level.
877	(m)1. Notwithstanding any other law, provide project
878	oversight on any information technology project of the
879	Department of Financial Services, the Department of Legal
880	Affairs, and the Department of Agriculture and Consumer Services
881	which has a total project cost of \$20 million or more. Such
882	information technology projects must also comply with the
883	applicable information technology architecture, project
884	management and oversight, and reporting standards established by
885	the department, acting through the Florida Digital Service.
886	2. When performing the project oversight function specified
887	in subparagraph 1., report at least quarterly to the Executive
888	Office of the Governor, the President of the Senate, and the
889	Speaker of the House of Representatives on any information
890	technology project that the department, acting through the
891	Florida Digital Service, identifies as high-risk due to the
892	project exceeding acceptable variance ranges defined and
893	documented in the project plan. The report shall include a risk
894	assessment, including fiscal risks, associated with proceeding
895	to the next stage of the project and a recommendation for
896	corrective actions required, including suspension or termination
897	of the project.
898	(n) If an information technology project implemented by a
899	state agency must be connected to or otherwise accommodated by

Page 31 of 111

576-02644-25 20257026 900 an information technology system administered by the Department 901 of Financial Services, the Department of Legal Affairs, or the 902 Department of Agriculture and Consumer Services, consult with these departments regarding the risks and other effects of such 903 904 projects on their information technology systems and work 905 cooperatively with these departments regarding the connections, 906 interfaces, timing, or accommodations required to implement such 907 projects. 908 (o) If adherence to standards or policies adopted by or 909 established pursuant to this section causes conflict with 910 federal regulations or requirements imposed on an entity within 911 the enterprise and results in adverse action against an entity 912 or federal funding, work with the entity to provide alternative 913 standards, policies, or requirements that do not conflict with 914 the federal regulation or requirement. The department, acting 915 through the Florida Digital Service, shall annually report such alternative standards to the Executive Office of the Governor, 916 917 the President of the Senate, and the Speaker of the House of 918 Representatives. 919 (p)1. Establish an information technology policy for all 920 information technology-related state contracts, including state 921 term contracts for information technology commodities, 922 consultant services, and staff augmentation services. The 923 information technology policy must include: 924 a. Identification of the information technology product and 92.5 service categories to be included in state term contracts. 926 b. Requirements to be included in solicitations for state 927 term contracts. 928 c. Evaluation criteria for the award of information

Page 32 of 111

CODING: Words stricken are deletions; words underlined are additions.

	576-02644-25 20257026
929	technology-related state term contracts.
930	d. The term of each information technology-related state
931	term contract.
932	e. The maximum number of vendors authorized on each state
933	term contract.
934	f. At a minimum, a requirement that any contract for
935	information technology commodities or services meet the National
936	Institute of Standards and Technology Cybersecurity Framework.
937	g. For an information technology project wherein project
938	oversight is required pursuant to paragraph (d) or paragraph
939	(m), a requirement that independent verification and validation
940	be employed throughout the project life cycle with the primary
941	objective of independent verification and validation being to
942	provide an objective assessment of products and processes
943	throughout the project life cycle. An entity providing
944	independent verification and validation may not have technical,
945	managerial, or financial interest in the project and may not
946	have responsibility for, or participate in, any other aspect of
947	the project.
948	2. Evaluate vendor responses for information technology-
949	related state term contract solicitations and invitations to
950	negotiate.
951	3. Answer vendor questions on information technology-
952	related state term contract solicitations.
953	4. Ensure that the information technology policy
954	established pursuant to subparagraph 1. is included in all
955	solicitations and contracts that are administratively executed
956	by the department.
957	(q) Recommend potential methods for standardizing data

Page 33 of 111

	576-02644-25 20257026
958	across state agencies which will promote interoperability and
959	reduce the collection of duplicative data.
960	(r) Recommend open data technical standards and
961	terminologies for use by the enterprise.
962	(s) Ensure that enterprise information technology solutions
963	are capable of utilizing an electronic credential and comply
964	with the enterprise architecture standards.
965	(2)(a) The Secretary of Management Services shall designate
966	a state chief information officer, who shall administer the
967	Florida Digital Service. The state chief information officer,
968	prior to appointment, must have at least 5 years of experience
969	in the development of information system strategic planning and
970	development or information technology policy, and, preferably,
971	have leadership-level experience in the design, development, and
972	deployment of interoperable software and data solutions.
973	(b) The state chief information officer, in consultation
974	with the Secretary of Management Services, shall designate a
975	state chief data officer. The chief data officer must be a
976	proven and effective administrator who must have significant and
977	substantive experience in data management, data governance,
978	interoperability, and security.
979	(3) The department, acting through the Florida Digital
980	Service and from funds appropriated to the Florida Digital
981	Service, shall:
982	(a) Create, not later than December 1, 2022, and maintain a
983	comprehensive indexed data catalog in collaboration with the
984	enterprise that lists the data elements housed within the
985	enterprise and the legacy system or application in which these
986	data elements are located. The data catalog must, at a minimum,
	Page 34 of 111

	576-02644-25 20257026
987	specifically identify all data that is restricted from public
988	disclosure based on federal or state laws and regulations and
989	require that all such information be protected in accordance
990	with s. 282.318.
991	(b) Develop and publish, not later than December 1, 2022,
992	in collaboration with the enterprise, a data dictionary for each
993	agency that reflects the nomenclature in the comprehensive
994	indexed data catalog.
995	(c) Adopt, by rule, standards that support the creation and
996	deployment of an application programming interface to facilitate
997	integration throughout the enterprise.
998	(d) Adopt, by rule, standards necessary to facilitate a
999	secure ecosystem of data interoperability that is compliant with
1000	the enterprise architecture.
1001	(e) Adopt, by rule, standards that facilitate the
1002	deployment of applications or solutions to the existing
1003	enterprise system in a controlled and phased approach.
1004	(f) After submission of documented use cases developed in
1005	conjunction with the affected agencies, assist the affected
1006	agencies with the deployment, contingent upon a specific
1007	appropriation therefor, of new interoperable applications and
1008	solutions:
1009	1. For the Department of Health, the Agency for Health Care
1010	Administration, the Agency for Persons with Disabilities, the
1011	Department of Education, the Department of Elderly Affairs, and
1012	the Department of Children and Families.
1013	2. To support military members, veterans, and their
1014	families.
1015	(4) For information technology projects that have a total
	Page 35 of 111

	576-02644-25 20257026
1016	project cost of \$10 million or more:
1017	(a) State agencies must provide the Florida Digital Service
1018	with written notice of any planned procurement of an information
1019	technology project.
1020	(b) The Florida Digital Service must participate in the
1021	development of specifications and recommend modifications to any
1022	planned procurement of an information technology project by
1023	state agencies so that the procurement complies with the
1024	enterprise architecture.
1025	(c) The Florida Digital Service must participate in post-
1026	award contract monitoring.
1027	(2) (5) The department, acting through the Florida Digital
1028	Service, may not retrieve or disclose any data without a shared-
1029	data agreement in place between the department and the
1030	enterprise entity that has primary custodial responsibility of,
1031	or data-sharing responsibility for, that data.
1032	(3) This section is repealed July 1, 2026.
1033	(6) The department, acting through the Florida Digital
1034	Service, shall adopt rules to administer this section.
1035	Section 10. <u>Section 282.00515</u> , Florida Statutes, is
1036	repealed.
1037	Section 11. Effective July 1, 2026, section 282.006,
1038	Florida Statutes, is created to read:
1039	282.006 Agency for State Systems and Enterprise Technology;
1040	duties; enterprise responsibilities; reporting
1041	(1) The Agency for State Systems and Enterprise Technology
1042	established in s. 20.70 shall operate as the state enterprise
1043	organization for information technology governance and is the
1044	lead entity responsible for understanding the unique state

Page 36 of 111
	576-02644-25 20257026
1045	agency information technology needs and environments, creating
1046	enterprise technology standards and strategy, supporting state
1047	agency technology efforts, and reporting on the status of
1048	technology for the enterprise.
1049	(2) The Legislature intends for ASSET policy, standards,
1050	guidance, and oversight to allow for adaptability to emerging
1051	technology and organizational needs while maintaining compliance
1052	with industry best practices. All policies, standards, and
1053	guidelines established pursuant to this chapter must be
1054	technology-agnostic and may not prescribe specific tools,
1055	platforms, or vendors.
1056	(3) ASSET shall establish the strategic direction of
1057	information technology in the state. ASSET shall develop and
1058	publish information technology policy that aligns with industry
1059	best practices for the management of the state's information
1060	technology resources. The policy must be updated as necessary to
1061	meet the requirements of this chapter and advancements in
1062	technology.
1063	(4) Related to its oversight of the state's technology
1064	enterprise, ASSET shall:
1065	(a) In coordination with state agency technology subject
1066	matter experts, develop, publish, and maintain an enterprise
1067	architecture that:
1068	1. Acknowledges the unique needs of the entities within the
1069	enterprise in the development and publication of standards and
1070	terminologies to facilitate digital interoperability;
1071	2. Supports the cloud-first policy as specified in s.
1072	<u>282.206;</u>
1073	3. Addresses how information technology infrastructure may
	Page 37 of 111

	576-02644-25 20257026
1074	be modernized to achieve security, scalability, maintainability,
1075	interoperability, and improved cost-efficiency goals; and
1076	4. Includes, at a minimum, best practices, guidelines, and
1077	standards for:
1078	a. Data models and taxonomies.
1079	b. Master data management.
1080	c. Data integration and interoperability.
1081	d. Data security and encryption.
1082	e. Bot prevention and data protection.
1083	f. Data backup and recovery.
1084	g. Application portfolio and catalog requirements.
1085	h. Application architectural patterns and principles.
1086	i. Technology and platform standards.
1087	j. Secure coding practices.
1088	k. Performance and scalability.
1089	1. Cloud infrastructure and architecture.
1090	m. Networking, connectivity, and security protocols.
1091	n. Authentication, authorization, and access controls.
1092	o. Disaster recovery.
1093	p. Quality assurance.
1094	q. Testing methodologies and measurements.
1095	r. Logging and log retention.
1096	s. Application and use of artificial intelligence.
1097	(b) Recommend open data technical standards and
1098	terminologies for use by the state's technology enterprise.
1099	(c) Develop enterprise technology testing and quality
1100	assurance best practices and standards to ensure the
1101	reliability, security, and performance of information technology
1102	systems. Such best practices and standards must include:

Page 38 of 111

	576-02644-25 20257026
1103	1. Functional testing to ensure software or systems meet
1104	required specifications.
1105	2. Performance and load testing to ensure software and
1106	systems operate efficiently under various conditions.
1107	3. Security testing to protect software and systems from
1108	vulnerabilities and cyber threats.
1109	4. Compatibility and interoperability testing to ensure
1110	software and systems operate seamlessly across environments.
1111	(5) ASSET shall produce the following reports and provide
1112	them to the Governor, the Commissioner of Agriculture, the Chief
1113	Financial Officer, the Attorney General, the President of the
1114	Senate, and the Speaker of the House of Representatives:
1115	(a) Annually by December 15, an enterprise analysis report
1116	that includes all of the following:
1117	1. Results of the state agency needs assessments, including
1118	any plan to address technical debt as required by s. 282.0061
1119	pursuant to the schedule adopted.
1120	2. Alternative standards related to federal funding adopted
1121	pursuant to s. 282.0061.
1122	3. Information technology financial data for each state
1123	agency for the previous fiscal year. This portion of the annual
1124	report must include, at a minimum, the following recurring and
1125	nonrecurring information:
1126	a. Total number of full-time equivalent positions.
1127	b. Total amount of salary.
1128	c. Total amount of benefits.
1129	d. Total number of comparable full-time equivalent
1130	positions and total amount of expenditures for information
1131	technology staff augmentation.

Page 39 of 111

	576-02644-25 20257026
1132	e. Total number of contracts and purchase orders and total
1133	amount of associated expenditures for information technology
1134	managed services.
1135	f. Total amount of expenditures by state term contract as
1136	defined in s. 287.012, contracts procured using alternative
1137	purchasing methods as authorized pursuant to s. 287.042(16), and
1138	state agency procurements through request for proposal,
1139	invitation to negotiate, invitation to bid, single source, and
1140	emergency purchases.
1141	g. Total amount of expenditures for hardware.
1142	h. Total amount of expenditures for non-cloud software.
1143	i. Total amount of expenditures for cloud software licenses
1144	and services with a separate amount for expenditures for state
1145	data center services.
1146	j. Total amount of expenditures for cloud data center
1147	services with a separate amount for expenditures for state data
1148	center services.
1149	k. Total amount of expenditures for administrative costs.
1150	4. Consolidated information for the previous fiscal year
1151	about state information technology projects, which must include,
1152	at a minimum, the following information:
1153	a. Anticipated funding requirements for information
1154	technology support over the next 5 years.
1155	b. An inventory of current information technology assets
1156	and major projects. The term "major project" includes projects
1157	costing more than \$500,000 to implement.
1158	c. Significant unmet needs for information technology
1159	resources over the next 5 fiscal years, ranked in priority order
1160	according to their urgency.

Page 40 of 111

CODING: Words stricken are deletions; words underlined are additions.

SB 7026

	576-02644-25 20257026
1161	5. A review and summary of whether the information
1162	technology contract policy established pursuant to s. 282.0064
1163	is included in all solicitations and contracts.
1164	6. Information related to the information technology test
1165	laboratory created in s. 282.0065, including usage statistics
1166	and key findings, and recommendations for improving the state's
1167	information technology procurement processes.
1168	(b) Biennially by December 15 of even-numbered years, a
1169	report on the strategic direction of information technology in
1170	the state which includes all of the following:
1171	1. Recommendations for standardization and consolidation of
1172	information technology services that are identified as common
1173	across state agencies as required in s. 282.0061.
1174	2. Recommendations for information technology services that
1175	should be designed, delivered, and managed as enterprise
1176	information technology services. Recommendations must include
1177	the identification of existing information technology resources
1178	associated with the services, if existing services must be
1179	transferred as a result of being delivered and managed as
1180	enterprise information technology services, and which entity is
1181	best suited to manage the service.
1182	(c)1. When conducted as provided in this paragraph, a
1183	market analysis and accompanying strategic plan submitted by
1184	December 31 of each year that the market analysis is conducted.
1185	2. No less frequently than every 3 years, ASSET shall
1186	conduct market analysis to determine whether the:
1187	a. Information technology resources within the enterprise
1188	are used in the most cost-effective and cost-efficient manner,
1189	while recognizing that the replacement of certain legacy

Page 41 of 111

	576-02644-25 20257026
1190	information technology systems within the enterprise may be cost
1191	prohibitive or cost inefficient due to the remaining useful life
1192	of those resources; and
1193	b. Enterprise is using best practices with respect to
1194	information technology, information services, and the
1195	acquisition of emerging technologies and information services.
1196	3. Each market analysis must be used to prepare a strategic
1197	plan for continued and future information technology and
1198	information services for the enterprise, including, but not
1199	limited to, proposed acquisition of new services or technologies
1200	and approaches to the implementation of any new services or
1201	technologies.
1202	(6) ASSET may adopt rules to implement this chapter.
1203	Section 12. Effective July 1, 2026, section 282.0061,
1204	Florida Statutes, is created to read:
1205	282.0061 ASSET support of state agencies; information
1206	technology procurement and projects
1207	(1) LEGISLATIVE INTENTThe Legislature intends for ASSET
1208	to support state agencies in their information technology
1209	efforts through the adoption of policies, standards, and
1210	guidance and by providing oversight that recognizes unique state
1211	agency information technology needs, environments, and goals.
1212	ASSET assistance and support must allow for adaptability to
1213	emerging technologies and organizational needs while maintaining
1214	compliance with industry best practices. ASSET may not prescribe
1215	specific tools, platforms, or vendors.
1216	(2) NEEDS ASSESSMENTS.—
1217	(a) By January 1, 2028, ASSET shall conduct full baseline
1218	needs assessments of state agencies to document their distinct

Page 42 of 111

	576-02644-25 20257026
1219	technical environments, existing technical debt, security risks,
1220	and compliance with all information technology standards and
1221	guidelines developed and published by ASSET. The needs
1222	assessment must use the Capability Maturity Model to evaluate
1223	each state agency's information technology capabilities,
1224	providing a maturity level rating for each assessed domain.
1225	After completion of the full baseline needs assessments, such
1226	assessments must be maintained and updated on a regular schedule
1227	adopted by ASSET.
1228	(b) In assessing the existing technical debt portion of the
1229	needs assessment, ASSET shall analyze the state's legacy
1230	information technology systems and develop a plan to document
1231	the needs and costs for replacement systems. The plan must
1232	include an inventory of legacy applications and infrastructure;
1233	the required capabilities not available with the legacy system;
1234	the estimated process, timeline, and cost to migrate from legacy
1235	environments; and any other information necessary for fiscal or
1236	technology planning. The plan must determine and document the
1237	estimated timeframe during which the state agency can continue
1238	to efficiently use legacy information technology systems,
1239	resources, security, and data management to support operations.
1240	State agencies shall provide all necessary documentation to
1241	enable accurate reporting on legacy systems.
1242	(c) ASSET shall develop a plan and schedule to conduct the
1243	initial full baseline needs assessments. By October 1, 2026,
1244	ASSET shall submit the plan to the Governor, the Commissioner of
1245	Agriculture, the Chief Financial Officer, the Attorney General,
1246	the President of the Senate, and the Speaker of the House of
1247	Representatives.

Page 43 of 111

	576-02644-25 20257026
1248	 (d) ASSET shall support state agency strategic planning
1249	efforts and assist state agencies with the production of a
1250	phased roadmap to address known technology gaps and deficiencies
1251	as identified in the needs assessments. The roadmaps must
1252	include specific strategies and initiatives aimed at advancing
1253	the state agency's maturity level in accordance with the
1254	Capability Maturity Model. State agencies shall create,
1255	maintain, and submit the roadmap on an annual basis with their
1256	legislative budget requests required under s. 216.023.
1257	(3) STANDARDIZATION.—ASSET shall:
1258	(a) Recommend in its annual enterprise analysis required
1259	under s. 282.006 any potential methods for standardizing data
1260	across state agencies which will promote interoperability and
1261	reduce the collection of duplicative data.
1262	(b) Identify any opportunities in its annual enterprise
1263	analysis required under s. 282.006 for standardization and
1264	consolidation of information technology services that are common
1265	across all state agencies and that support:
1266	1. Improved interoperability, security, scalability,
1267	maintainability, and cost efficiency; and
1268	2. Business functions and operations, including
1269	administrative functions such as purchasing, accounting and
1270	reporting, cash management, and personnel.
1271	(4) DATA MANAGEMENT.—
1272	(a) ASSET shall develop standards for use by state agencies
1273	which support best practices for master data management at the
1274	state agency level to facilitate enterprise data sharing and
1275	interoperability.
1276	(b) ASSET shall establish a methodology and strategy for

Page 44 of 111

	576-02644-25 20257026
1277	implementing statewide master data management and submit a
1278	report to the Governor, the Commissioner of Agriculture, the
1279	Chief Financial Officer, the Attorney General, the President of
1280	the Senate, and the Speaker of the House of Representatives by
1281	December 1, 2028. The report must include the vision, goals, and
1282	benefits of implementing a statewide master data management
1283	initiative, an analysis of the current state of data management,
1284	and the recommended strategy, methodology, and estimated
1285	timeline and resources needed at a state agency and enterprise
1286	level to accomplish the initiative.
1287	(5) INFORMATION TECHNOLOGY PROJECTSASSET has the
1288	following duties and responsibilities related to state agency
1289	technology projects:
1290	(a) Provide procurement advisory and review services for
1291	information technology projects to all state agencies, including
1292	procurement and contract development assistance to meet the
1293	information technology contract policy established pursuant to
1294	<u>s. 282.0064.</u>
1295	(b) Establish best practices and enterprise procurement
1296	processes and develop metrics to support these processes for the
1297	procurement of information technology products and services in
1298	order to reduce costs or improve the provision of government
1299	services.
1300	(c) Upon request, assist state agencies in the development
1301	of information technology-related legislative budget requests.
1302	(d) Develop standards and accountability measures for
1303	information technology projects, including criteria for
1304	effective project management and oversight. State agencies must
1305	satisfy these standards and measures when implementing

Page 45 of 111

	576-02644-25 20257026
1306	information technology projects. To support data-driven
1307	decisionmaking, the standards and measures must include, but are
1308	not limited to:
1309	1. Performance measurements and metrics that objectively
1310	reflect the status of an information technology project based on
1311	a defined and documented project scope, to include the volume of
1312	impacted stakeholders, cost, and schedule.
1313	2. Methodologies for calculating and defining acceptable
1314	variances in the projected versus actual scope, schedule, or
1315	cost of an information technology project.
1316	3. Reporting requirements designed to alert all defined
1317	stakeholders that an information technology project has exceeded
1318	acceptable variances defined and documented in a project plan as
1319	well as any variances that represent a schedule delay of 1 month
1320	or more or a cost increase of \$1 million or more.
1321	4. Technical standards to ensure an information technology
1322	project complies with the enterprise architecture standards.
1323	(e) Develop information technology project reports for use
1324	by state agencies, including, but not limited to, operational
1325	work plans, project spending plans, and project status reports.
1326	Reporting standards must include content, format, and frequency
1327	of project updates.
1328	(f) Provide training opportunities to state agencies to
1329	assist in the adoption of the project management and oversight
1330	standards.
1331	(g) Perform project oversight on all state agency
1332	information technology projects that have total project costs of
1333	\$10 million or more. ASSET shall report by the 30th day after
1334	the end of each quarter to the Executive Office of the Governor,

Page 46 of 111

1	576-02644-25 20257026
1335	the Commissioner of Agriculture, the Chief Financial Officer,
1336	the Attorney General, the President of the Senate, and the
1337	Speaker of the House of Representatives on any information
1338	technology project that ASSET identifies as high-risk. The
1339	report must include a risk assessment, including fiscal risks,
1340	associated with proceeding to the next stage of the project, and
1341	a recommendation for corrective actions required, including
1342	suspension or termination of the project.
1343	(h) Establish a streamlined reporting process with clear
1344	timelines and escalation procedures for notifying a state agency
1345	of noncompliance with the standards developed and adopted by
1346	ASSET.
1347	(6) INFORMATION TECHNOLOGY FINANCIAL DATA
1348	(a) In consultation with state agencies, ASSET shall create
1349	a methodology, an approach, and applicable templates and formats
1350	for identifying and collecting both current and planned
1351	information technology expenditure data at the state agency
1352	level. ASSET shall continuously obtain, review, and maintain
1353	records of the appropriations, expenditures, and revenues for
1354	information technology for each state agency.
1355	(b) ASSET shall prescribe the format for state agencies to
1356	provide all necessary financial information to ASSET for
1357	inclusion in the annual report required under s. 282.006. State
1358	agencies must provide the information to ASSET by October 1 for
1359	the previous fiscal year. The information must be reported by
1360	ASSET in order to determine all costs and expenditures for
1361	information technology assets and resources provided by the
1 2 6 0	
1362	state agencies or through contracts or grants.

Page 47 of 111

	576-02644-25 20257026
1364	to provide alternative standards, policies, or requirements that
1365	do not conflict with federal regulations or requirements if
1366	adherence to standards or policies adopted by or established
1367	pursuant to this section conflict with federal regulations or
1368	requirements imposed on an entity within the enterprise and
1369	results in, or is expected to result in, adverse action against
1370	the state agencies or loss of federal funding.
1371	Section 13. Effective July 1, 2026, section 282.0062,
1372	Florida Statutes, is created to read:
1373	282.0062 ASSET workgroupsThe following workgroups are
1374	established within ASSET to facilitate coordination with state
1375	agencies:
1376	(1) CHIEF INFORMATION OFFICER WORKGROUP
1377	(a) The chief information officer workgroup, composed of
1378	all state agency chief information officers, shall consider and
1379	make recommendations to the state chief information officer and
1380	the state chief information architect on such matters as
1381	enterprise information technology policies, standards, services,
1382	and architecture. The workgroup may also identify and recommend
1383	opportunities for the establishment of public-private
1384	partnerships when considering technology infrastructure and
1385	services in order to accelerate project delivery and provide a
1386	source of new or increased project funding.
1387	(b) At a minimum, the state chief information officer shall
1388	consult with the workgroup on a quarterly basis with regard to
1389	executing the duties and responsibilities of the state agencies
1390	related to statewide information technology strategic planning
1391	and policy.
1392	(2) ENTERPRISE DATA AND INTEROPERABILITY WORKGROUP

Page 48 of 111

	576-02644-25 20257026
1393	(a) The enterprise data and interoperability workgroup,
1394	composed of chief data officer representatives from all state
1395	agencies, shall consider and make recommendations to the state
1396	chief data officer on such matters as enterprise data policies,
1397	standards, services, and architecture that promote data
1398	consistency, accessibility, and seamless integration across the
1399	enterprise.
1400	(b) At a minimum, the state chief data officer shall
1401	consult with the workgroup on a quarterly basis with regard to
1402	executing the duties and responsibilities of the state agencies
1403	related to statewide data governance planning and policy.
1404	(3) ENTERPRISE SECURITY WORKGROUP
1405	(a) The enterprise security workgroup, composed of chief
1406	information security officer representatives from all state
1407	agencies, shall consider and make recommendations to the state
1408	chief information security officer on such matters as
1409	cybersecurity policies, standards, services, and architecture
1410	that promote the protection of state assets.
1411	(b) At a minimum, the state chief information security
1412	officer shall consult with the workgroup on a quarterly basis
1413	with regard to executing the duties and responsibilities of the
1414	state agencies related to cybersecurity governance and policy
1415	development.
1416	(4) ENTERPRISE INFORMATION TECHNOLOGY OPERATIONS
1417	WORKGROUP
1418	(a) The enterprise information technology operations
1419	workgroup, composed of information technology business analyst
1420	representatives from all state agencies, shall consider and make
1421	recommendations to the state chief technology officer on such

Page 49 of 111

	576-02644-25 20257026
1422	matters as information technology needs assessments policies,
1423	standards, and services that promote the strategic alignment of
1424	technology with operational needs and the evaluation of
1425	solutions across the enterprise.
1426	(b) At a minimum, the state chief technology officer shall
1427	consult with the workgroup on a quarterly basis with regard to
1428	executing the duties and responsibilities of the state agencies
1429	related to statewide process improvement and optimization.
1430	(5) ENTERPRISE INFORMATION TECHNOLOGY QUALITY ASSURANCE
1431	WORKGROUP
1432	(a) The enterprise information technology quality assurance
1433	workgroup, composed of testing and quality assurance
1434	representatives from all state agencies, shall consider and make
1435	recommendations to the state chief technology officer on such
1436	matters as testing methodologies, tools, and best practices to
1437	reduce risks related to software defects, cybersecurity threats,
1438	and operational failures.
1439	(b) At a minimum, the state chief technology officer shall
1440	consult with the workgroup on a quarterly basis with regard to
1441	executing the duties and responsibilities of the state agencies
1442	related to enterprise software testing and quality assurance
1443	standards.
1444	(6) ENTERPRISE INFORMATION TECHNOLOGY PROJECT MANAGEMENT
1445	WORKGROUP
1446	(a) The enterprise information technology project
1447	management workgroup, composed of information technology project
1448	manager representatives from all state agencies, shall consider
1449	and make recommendations to the state chief technology officer
1450	on such matters as information technology project management

Page 50 of 111

	576-02644-25 20257026
1451	policies, standards, accountability measures, and services that
1452	promote project governance and standardization across the
1453	enterprise.
1454	(b) At a minimum, the state chief technology officer shall
1455	consult with the workgroup on a quarterly basis with regard to
1456	executing the duties and responsibilities of the state agencies
1457	related to project management and oversight.
1458	(7) ENTERPRISE INFORMATION TECHNOLOGY CONTRACT MANAGEMENT
1459	WORKGROUP
1460	(a) The enterprise information technology contract
1461	management workgroup, composed of information technology
1462	contract manager representatives from all state agencies, shall
1463	consider and make recommendations to the state chief technology
1464	officer on such matters as information technology contract
1465	management policies and standards that promote best practices
1466	for vendor oversight, risk management and compliance, and
1467	performance monitoring and reporting across the enterprise.
1468	(b) At a minimum, the state chief technology officer shall
1469	consult with the workgroup on a quarterly basis with regard to
1470	executing the duties and responsibilities of the state agencies
1471	related to contract management and vendor accountability.
1472	(8) ENTERPRISE INFORMATION TECHNOLOGY PURCHASING
1473	WORKGROUP
1474	(a) The enterprise information technology purchasing
1475	workgroup, composed of information technology procurement
1476	representatives from all state agencies, shall consider and make
1477	recommendations to the state chief information technology
1478	procurement officer on such matters as information technology
1479	procurement policies, standards, and purchasing strategy and

Page 51 of 111

1	576-02644-25 20257026
1480	optimization that promote best practices for contract
1481	negotiation, consolidation, and effective service-level
1482	agreement implementation across the enterprise.
1483	(b) At a minimum, the state chief information technology
1484	procurement officer shall consult with the workgroup on a
1485	quarterly basis with regard to executing the duties and
1486	responsibilities of the state agencies related to technology
1487	evaluation, purchasing, and cost savings.
1488	Section 14. Effective July 1, 2026, section 282.0063,
1489	Florida Statutes, is created to read:
1490	282.0063 State information technology professionals career
1491	paths and training
1492	(1) ASSET shall develop standardized frameworks for, and
1493	career paths, progressions, and training programs for, the
1494	benefit of state agency information technology personnel. To
1495	meet that goal, ASSET shall:
1496	(a) Assess current and future information technology
1497	workforce needs across state agencies, identifying skill gaps
1498	and developing strategies to address them.
1499	(b) Develop and establish a training program for state
1500	agencies to support the understanding and implementation of each
1501	element of the enterprise architecture.
1502	(c) Establish training programs, certifications, and
1503	continuing education opportunities to enhance information
1504	technology competencies, including cybersecurity, cloud
1505	computing, and emerging technologies.
1506	(d) Support initiatives to upskill existing employees in
1507	emerging technologies and automation, ensuring state agencies
1508	remain competitive and innovative.

Page 52 of 111

	576-02644-25 20257026
1509	(e) Develop strategies to recruit and retain information
1510	technology professionals, including internship programs,
1511	partnerships with educational institutions, scholarships for
1512	service, and initiatives to attract diverse talent.
1513	(2) ASSET shall consult with CareerSource Florida, Inc.,
1514	the Department of Commerce, and the Department of Education in
1515	the implementation of this section.
1516	(3) Specifically, in consultation with the Division of
1517	State Human Resource Management in the Department of Management
1518	Services, ASSET shall:
1519	(a) Define career progression frameworks for information
1520	technology personnel, for supporting leadership development, and
1521	for providing mentorship programs.
1522	(b) Establish guidelines and best practices for information
1523	technology professional development and performance management
1524	across state agencies.
1525	Section 15. Effective July 1, 2026, section 282.0064,
1526	Florida Statutes, is created to read:
1527	282.0064 Information technology contract policy
1528	(1) In coordination with the Department of Management
1529	Services, ASSET shall establish a policy for all information
1530	technology-related solicitations and contracts, including state
1531	term contracts; contracts sourced using alternative purchasing
1532	methods as authorized pursuant to s. 287.042(16); sole source
1533	and emergency procurements; and contracts for commodities,
1534	consultant services, and staff augmentation services.
1535	(2) Related to state term contracts, the information
1536	technology policy must include:
1537	(a) Identification of the information technology product

Page 53 of 111

	576-02644-25 20257026
1538	and service categories to be included in state term contracts.
1539	(b) The term of each information technology-related state
1540	term contract.
1541	(c) The maximum number of vendors authorized on each state
1542	term contract.
1543	(3) For all contracts, the information technology policy
1544	must include:
1545	(a) Evaluation criteria for the award of information
1546	technology-related contracts.
1547	(b) Requirements to be included in solicitations.
1548	(c) At a minimum, a requirement that any contract for
1549	information technology commodities or services must meet the
1550	requirements of the enterprise architecture and National
1551	Institute of Standards and Technology Cybersecurity Framework.
1552	(4) The policy must include the following requirements for
1553	any information technology project that requires project
1554	oversight through independent verification and validation:
1555	(a) An entity providing independent verification and
1556	validation may not have any:
1557	1. Technical, managerial, or financial interest in the
1558	project; or
1559	2. Responsibility for or participation in any other aspect
1560	of the project.
1561	(b) The primary objective of independent verification and
1562	validation must be to provide an objective assessment throughout
1563	the entire project life cycle, reporting directly to all
1564	relevant stakeholders. An independent verification and
1565	validation entity shall independently verify and validate
1566	whether:

Page 54 of 111

	576-02644-25 20257026
1567	1. The project is being built and implemented in accordance
1568	with defined technical architecture, specifications, and
1569	requirements.
1570	2. The project is adhering to established project
1571	management processes.
1572	3. The procurement of products, tools, and services and
1573	resulting contracts align with current statutory and regulatory
1574	requirements.
1575	4. The value of services delivered is commensurate with
1576	project costs.
1577	5. The completed project meets the actual needs of the
1578	intended users.
1579	(c) The entity performing independent verification and
1580	validation shall provide regular reports and assessments
1581	directly to the designated oversight body, identifying risks,
1582	deficiencies, and recommendations for corrective actions to
1583	ensure project success and compliance with statutory
1584	requirements.
1585	(5) The Division of State Purchasing in the Department of
1586	Management Services shall coordinate with ASSET on state term
1587	contract solicitations and invitations to negotiate related to
1588	information technology. ASSET shall evaluate vendor responses
1589	and answer vendor questions on such solicitations or invitations
1590	to negotiate.
1591	Section 16. Effective July 1, 2026, section 282.0065,
1592	Florida Statutes, is created to read:
1593	282.0065 ASSET information technology test laboratory
1594	(1) Beginning July 1, 2027, or after all elements of the
1595	enterprise architecture are published, whichever is later, and
I	

Page 55 of 111

	576-02644-25 20257026
1596	subject to specific appropriation, ASSET shall establish,
1597	maintain, and manage an information technology test laboratory
1598	to support state agencies in evaluating information technology
1599	services, software, and tools before procurement and
1600	implementation.
1601	(2) The purpose of the information technology test
1602	laboratory is to:
1603	(a) Serve as an independent environment for state agencies
1604	to develop, test, and refine proofs of concept for information
1605	technology solutions to assess functionality, security,
1606	interoperability, and performance; and
1607	(b) Assist state agencies in defining and improving
1608	procurement requirements based on real-world testing and
1609	evaluation.
1610	(3) ASSET shall:
1611	(a) Operate and maintain the test laboratory and ensure
1612	that it remains fully operational with the necessary
1613	infrastructure, resources, and security controls to support
1614	state agency testing activities.
1615	(b) Facilitate proofs of concept for state agencies by
1616	providing the agencies with controlled environments to assess
1617	emerging technologies, validate vendor claims, and conduct
1618	comparative evaluations of information technology solutions.
1619	(c) Support the development of requirements for state
1620	agency information technology projects by assisting state
1621	agencies in refining technical specifications, performance
1622	benchmarks, and security requirements prior to issuing
1623	procurement solicitations.
1624	(d) Ensure the security and compliance of the test

Page 56 of 111

	576-02644-25 20257026
1625	laboratory by implementing safeguards to protect sensitive data,
1626	ensure compliance with applicable laws, and prevent unauthorized
1627	access to testing environments.
1628	(e) Provide access to emerging technologies by partnering
1629	with industry and research institutions to ensure that state
1630	agencies have the opportunity to evaluate the latest information
1631	technology innovations relevant to government operations.
1632	(f) Enter into partnerships with public and private
1633	entities to support the information technology test laboratory's
1634	operations, provided that such partnerships comply with
1635	conflict-of-interest policies and procurement regulations.
1636	(g) Establish policies, procedures, and eligibility
1637	criteria for state agencies to access and use the lab.
1638	Section 17. Section 282.0066, Florida Statutes, is created
1639	to read:
1640	282.0066 Enterprise Information Technology Library
1641	(1) ASSET shall develop, implement, and maintain a library
1642	to serve as the official repository for all enterprise
1643	information technology policies, standards, guidelines, and best
1644	practices applicable to state agencies. The library must be
1645	online and accessible by all state agencies through a secure
1646	authentication system.
1647	(2) In developing the library, ASSET shall create a
1648	structured index and search functionality to facilitate
1649	efficient retrieval of information and maintain version control
1650	and revision history for all published documents.
1651	(3) The library must include standardized checklists
1652	organized by technical subject areas to assist state agencies in
1653	measuring compliance with the information technology policies,

Page 57 of 111

	576-02644-25 20257026
1654	standards, guidelines, and best practices.
1655	(4) ASSET shall establish procedures to ensure the
1656	integrity, security, and availability of the library, including
1657	appropriate access controls, encryption, and disaster recovery
1658	measures. ASSET must regularly update documents and materials of
1659	the library to reflect current state and federal requirements,
1660	industry best practices, and emerging technologies.
1661	(5)(a) All state agencies shall reference and adhere to the
1662	policies, standards, guidelines, and best practices contained in
1663	the online library in information technology planning,
1664	procurement, implementation, and operations. ASSET shall create
1665	mechanisms for state agencies to submit feedback, request
1666	clarifications, and recommend updates.
1667	(b)1. A state agency may request an exemption to a specific
1668	policy, standard, or guideline when compliance is not
1669	technically feasible, would cause undue hardship, or conflicts
1670	with agency specific statutory requirements. The state agency
1671	requesting an exception must submit a formal justification to
1672	ASSET detailing all of the following:
1673	a. The specific requirement for which an exemption is
1674	sought.
1675	b. The reason compliance is not feasible or practical.
1676	c. Any compensating controls or alternative measures the
1677	state agency will implement to mitigate associated risks.
1678	d. The anticipated duration of the exemption.
1679	2. ASSET shall review all exemption requests and provide a
1680	recommendation to the state chief information officer who shall
1681	present the compliance exemption requests to the chief
1682	information officer workgroup. Approval of exemption requests

Page 58 of 111

	576-02644-25 20257026
1683	must be made by a majority vote of the workgroup. Approved
1684	exemptions must be documented, including conditions and
1685	expiration dates.
1686	3. A state agency with an approved exemption must undergo
1687	periodic review to determine whether the exemption remains
1688	necessary or if compliance can be achieved.
1689	Section 18. Paragraphs (b), (c), (g), (h), and (i) of
1690	subsection (3) and paragraphs (b), (c), (d), and (j) of
1691	subsection (3) and paragraphs (b), (c), (d), and (j) of subsection (4) of section 282.318, Florida Statutes, are amended
1692	to read:
1693	282.318 Cybersecurity
1694	
1695	
	Service, is the lead entity responsible for establishing
1696	standards and processes for assessing state agency cybersecurity
1697	risks and determining appropriate security measures. Such
1698	standards and processes must be consistent with generally
1699	accepted technology best practices, including the National
1700	Institute for Standards and Technology Cybersecurity Framework,
1701	for cybersecurity. The department, acting through the Florida
1702	Digital Service, shall adopt rules that mitigate risks;
1703	safeguard state agency digital assets, data, information, and
1704	information technology resources to ensure availability,
1705	confidentiality, and integrity; and support a security
1706	governance framework. The department, acting through the Florida
1707	Digital Service, shall also:
1708	(b) Develop, and annually update by February 1, a statewide
1709	cybersecurity strategic plan that includes security goals and
1710	objectives for cybersecurity, including the identification and
1711	mitigation of risk, proactive protections against threats,

Page 59 of 111

	576-02644-25 20257026
1712	tactical risk detection, threat reporting, and response and
1713	recovery protocols for a cyber incident.
1714	(c) Develop and publish for use by state agencies a
1715	cybersecurity governance framework that, at a minimum, includes
1716	guidelines and processes for:
1717	1. Establishing asset management procedures to ensure that
1718	an agency's information technology resources are identified and
1719	managed consistent with their relative importance to the
1720	agency's business objectives.
1721	2. Using a standard risk assessment methodology that
1722	includes the identification of an agency's priorities,
1723	constraints, risk tolerances, and assumptions necessary to
1724	support operational risk decisions.
1725	3. Completing comprehensive risk assessments and
1726	cybersecurity audits, which may be completed by a private sector
1727	vendor, and submitting completed assessments and audits to the
1728	department.
1729	4. Identifying protection procedures to manage the
1730	protection of an agency's information, data, and information
1731	technology resources.
1732	5. Establishing procedures for accessing information and
1733	data to ensure the confidentiality, integrity, and availability
1734	of such information and data.
1735	6. Detecting threats through proactive monitoring of
1736	events, continuous security monitoring, and defined detection
1737	processes.
1738	7. Establishing agency cybersecurity incident response
1739	teams and describing their responsibilities for responding to
1740	cybersecurity incidents, including breaches of personal
I	

Page 60 of 111

1742 1743 1744 1745 1746 1747 1748 a. 1749 1750 1751 1752 1753

576-02644-25

1741

```
20257026
```

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

information containing confidential or exempt data.

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

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

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

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

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

1764 (IV) Level 2 is a medium-level incident that may impact 1765 public health or safety; national, state, or local security; 1766 economic security; civil liberties; or public confidence.

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

Page 61 of 111

	576-02644-25 20257026
1770	confidence.
1771	b. The cybersecurity incident reporting process must
1772	specify the information that must be reported by a state agency
1773	following a cybersecurity incident or ransomware incident,
1774	which, at a minimum, must include the following:
1775	(I) A summary of the facts surrounding the cybersecurity
1776	incident or ransomware incident.
1777	(II) The date on which the state agency most recently
1778	backed up its data; the physical location of the backup, if the
1779	backup was affected; and if the backup was created using cloud
1780	computing.
1781	(III) The types of data compromised by the cybersecurity
1782	incident or ransomware incident.
1783	(IV) The estimated fiscal impact of the cybersecurity
1784	incident or ransomware incident.
1785	(V) In the case of a ransomware incident, the details of
1786	the ransom demanded.
1787	c.(I) A state agency shall report all ransomware incidents
1788	and any cybersecurity incident determined by the state agency to
1789	be of severity level 3, 4, or 5 to the state chief information
1790	security officer Cybersecurity Operations Center and the
1791	Cybercrime Office of the Department of Law Enforcement as soon
1792	as possible but no later than 48 hours after discovery of the
1793	cybersecurity incident and no later than 12 hours after
1794	discovery of the ransomware incident. The report must contain
1795	the information required in sub-subparagraph b.
1796	(II) The state chief information security officer
1797	Cybersecurity Operations Center shall notify the President of
1798	the Senate and the Speaker of the House of Representatives of

Page 62 of 111

	576-02644-25 20257026
1799	any severity level 3, 4, or 5 incident as soon as possible but
1800	no later than 12 hours after receiving a state agency's incident
1801	report. The notification must include a high-level description
1802	of the incident and the likely effects.
1803	d. A state agency shall report a cybersecurity incident
1804	determined by the state agency to be of severity level 1 or 2 to
1805	the state chief information security officer Cybersecurity
1806	Operations Center and the Cybercrime Office of the Department of
1807	Law Enforcement as soon as possible, but no later than 96 hours
1808	after the discovery of the cybersecurity incident and no later
1809	than 72 hours after the discovery of the ransomware incident.
1810	The report must contain the information required in sub-
1811	subparagraph b.
1812	e. The state chief information security officer
1813	Cybersecurity Operations Center shall provide a consolidated
1814	incident report on a quarterly basis to the President of the
1815	Senate ${ m and}_{ au}$ the Speaker of the House of Representatives, and the
1816	Florida Cybersecurity Advisory Council. The report provided to
1817	the Florida Cybersecurity Advisory Council may not contain the
1818	name of any agency, network information, or system identifying
1819	information but must contain sufficient relevant information to
1820	allow the Florida Cybersecurity Advisory Council to fulfill its
1821	responsibilities as required in s. 282.319(9).
1822	2.10. Incorporating information obtained through detection
1823	and response activities into the agency's cybersecurity incident
1824	response plans.
1825	3.11. Developing agency strategic and operational
1826	avborsocurity plans required pursuant to this section

1826 cybersecurity plans required pursuant to this section.

1827

4.12. Establishing the managerial, operational, and

Page 63 of 111

576-02644-25

1828	technical safeguards for protecting state government data and
1829	information technology resources that align with the state
1830	agency risk management strategy and that protect the
1831	confidentiality, integrity, and availability of information and
1832	data.
1833	13. Establishing procedures for procuring information
1834	technology commodities and services that require the commodity
1835	or service to meet the National Institute of Standards and
1836	Technology Cybersecurity Framework.
1837	5.14. Submitting after-action reports following a
1838	cybersecurity incident or ransomware incident. Such guidelines
1839	and processes for submitting after-action reports must be
1840	developed and published by December 1, 2022.
1841	<u>(f)</u> Annually provide cybersecurity training to all state
1842	agency technology professionals and employees with access to
1843	highly sensitive information which develops, assesses, and
1844	documents competencies by role and skill level. The
1845	cybersecurity training curriculum must include training on the
1846	identification of each cybersecurity incident severity level
1847	referenced in sub-subparagraph <u>(b)1.a.</u> (c)9.a. The training may
1848	be provided in collaboration with the Cybercrime Office of the
1849	Department of Law Enforcement, a private sector entity, or an
1850	institution of the State University System.
1851	(h) Operate and maintain a Cybersecurity Operations Center
1852	led by the state chief information security officer, which must
1853	be primarily virtual and staffed with tactical detection and
1854	incident response personnel. The Cybersecurity Operations Center

- 1855 shall serve as a clearinghouse for threat information and
- 1856 coordinate with the Department of Law Enforcement to support

Page 64 of 111

CODING: Words stricken are deletions; words underlined are additions.

20257026

576-02644-25

```
1857
      state agencies and their response to any confirmed or suspected
1858
      cybersecurity incident.
1859
           (i) Lead an Emergency Support Function, ESF CYBER, under
1860
      the state comprehensive emergency management plan as described
1861
      in s. 252.35.
1862
            (4) Each state agency head shall, at a minimum:
1863
            (b)
                In consultation with the department, through the
1864
      Florida Digital Service, and the Cybercrime Office of the
      Department of Law Enforcement, establish an agency cybersecurity
1865
1866
      response team to respond to a cybersecurity incident. The agency
1867
      cybersecurity response team shall convene upon notification of a
1868
      cybersecurity incident and must immediately report all confirmed
1869
      or suspected incidents to the state chief information security
1870
      officer, or his or her designee, and comply with all applicable
1871
      guidelines and processes established pursuant to paragraph
1872
      (3)(b) <del>(3)(c)</del>.
1873
            (c) Submit to the state chief information security officer
1874
      department annually by July 31_7 the state agency's strategic and
1875
      operational cybersecurity plans developed pursuant to rules and
1876
      guidelines established by the state chief information security
1877
      officer department, through the Florida Digital Service.
1878
           1. The state agency strategic cybersecurity plan must cover
1879
      a 2-year 3-year period and, at a minimum, define security goals,
1880
      intermediate objectives, and projected agency costs for the
      strategic issues of agency information security policy, risk
1881
1882
      management, security training, security incident response, and
1883
      disaster recovery. The plan must be based on the statewide
1884
      cybersecurity strategic plan created by the state chief
      information security officer department and include performance
1885
```

Page 65 of 111

CODING: Words stricken are deletions; words underlined are additions.

20257026

576-02644-25 20257026 1886 metrics that can be objectively measured to reflect the status 1887 of the state agency's progress in meeting security goals and 1888 objectives identified in the agency's strategic information 1889 security plan. 1890 2. The state agency operational cybersecurity plan must 1891 include a set of measures that objectively assesses the 1892 performance of the agency's cybersecurity program in accordance 1893 with its risk management plan progress report that objectively 1894 measures progress made towards the prior operational 1895 cybersecurity plan and a project plan that includes activities, 1896 timelines, and deliverables for security objectives that the 1897 state agency will implement during the current fiscal year. 1898 (d) Conduct, and update every 2 - 3 years, a comprehensive 1899 risk assessment, which may be completed by a private sector 1900 vendor, to determine the security threats to the data, 1901 information, and information technology resources, including 1902 mobile devices and print environments, of the agency. The risk 1903 assessment must comply with the risk assessment methodology 1904 developed by the state chief information security officer 1905 department and is confidential and exempt from s. 119.07(1), 1906 except that such information shall be available to the Auditor 1907 General, the state chief information security officer Florida 1908 Digital Service within the department, the Cybercrime Office of 1909 the Department of Law Enforcement, and, for state agencies under 1910 the jurisdiction of the Governor, the Chief Inspector General. 1911 If a private sector vendor is used to complete a comprehensive 1912 risk assessment, it must attest to the validity of the risk 1913 assessment findings. The comprehensive risk assessment must 1914 include all of the following:

Page 66 of 111

	576-02644-25 20257026
1915	1. The results of vulnerability and penetration tests on
1916	any Internet website or mobile application that processes any
1917	sensitive personal information or confidential information and a
1918	plan to address any vulnerability identified in the tests.
1919	2. A written acknowledgment that the executive director or
1920	the secretary of the agency, the chief financial officer of the
1921	agency, and each executive manager as designated by the state
1922	agency have been made aware of the risks revealed during the
1923	preparation of the agency's operations cybersecurity plan and
1924	the comprehensive risk assessment.
1925	(j) Develop a process for detecting, reporting, and
1926	responding to threats, breaches, or cybersecurity incidents
1927	which is consistent with the security rules, guidelines, and
1928	processes established by the department through the Florida
1929	Digital Service.
1930	1. All cybersecurity incidents and ransomware incidents
1931	must be reported by state agencies. Such reports must comply
1932	with the notification procedures and reporting timeframes
1933	established pursuant to paragraph $(3)(b)$ $(3)(c)$.
1934	2. For cybersecurity breaches, state agencies shall provide
1935	notice in accordance with s. 501.171.
1936	Section 19. Effective July 1, 2026, subsections (2), (3),
1937	(4), (7), and (10) of section 282.318, Florida Statutes, as
1938	amended by this act, are amended to read:
1939	282.318 Cybersecurity
1940	(2) As used in this section, the term "state agency" has
1941	the same meaning as provided in s. 282.0041, except that the
1942	term includes the Department of Legal Affairs, the Department of
1943	Agriculture and Consumer Services, and the Department of
I	Page 67 of 111

576-02644-25

1944 Financial Services.

1945 (3) ASSET The department, acting through the Florida 1946 Digital Service, is the lead entity responsible for establishing 1947 enterprise technology and cybersecurity standards and processes 1948 for assessing state agency cybersecurity risks and determining appropriate security measures that comply with all national and 1949 1950 state data compliance security standards. Such standards and 1951 processes must be consistent with generally accepted technology 1952 best practices, including the National Institute for Standards 1953 and Technology Cybersecurity Framework, for cybersecurity. ASSET 1954 The department, acting through the Florida Digital Service, 1955 shall adopt rules that mitigate risks; safequard state agency 1956 digital assets, data, information, and information technology 1957 resources to ensure availability, confidentiality, and 1958 integrity; and support a security governance framework. ASSET 1959 The department, acting through the Florida Digital Service, 1960 shall also:

1961 (a) Designate an employee of the Florida Digital Service as 1962 the state chief information security officer. The state chief 1963 information security officer must have experience and expertise 1964 in security and risk management for communications and 1965 information technology resources. The state chief information 1966 security officer is responsible for the development of 1967 enterprise cybersecurity policy, standards, operation, and security architecture oversight of cybersecurity for state 1968 1969 technology systems. The state chief information security officer 1970 shall be notified of all confirmed or suspected incidents or 1971 threats of state agency information technology resources and 1972 must report such incidents or threats to the state chief

Page 68 of 111

CODING: Words stricken are deletions; words underlined are additions.

20257026

	576-02644-25 20257026
1973	information officer and the Governor.
1974	(b) Develop, and annually update by February 1, a statewide
1975	cybersecurity strategic plan that includes security goals and
1976	objectives for cybersecurity, including the identification and
1977	mitigation of risk, proactive protections against threats,
1978	tactical risk detection, threat reporting, and response and
1979	recovery protocols for a cyber incident.
1980	<u>(c) (b)</u> Develop and publish for use by state agencies a
1981	cybersecurity governance framework that, at a minimum, includes
1982	guidelines and processes for:
1983	1. Establishing asset management procedures to ensure that
1984	an agency's information technology resources are identified and
1985	managed consistently with their relative importance to the
1986	agency's business objectives.
1987	2. Using a standard risk assessment methodology that
1988	includes the identification of an agency's priorities,
1989	constraints, risk tolerances, and assumptions necessary to
1990	support operational risk decisions.
1991	3. Completing comprehensive risk assessments and
1992	cybersecurity audits, which may be completed by a private sector
1993	vendor, and submitting completed assessments and audits to the
1994	department.
1995	4. Identifying protection procedures to manage the
1996	protection of an agency's information, data, and information
1997	technology resources.
1998	5. Establishing procedures for accessing information and
1999	data to ensure the confidentiality, integrity, and availability
2000	of such information and data.
2001	6. Detecting threats through proactive monitoring of

Page 69 of 111

576-02644-25

20257026

02 <u>events</u>, continuous security monitoring, and defined detection 03 processes.

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

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

<u>9.</u> Establishing a cybersecurity incident reporting process that includes procedures for notifying <u>ASSET</u> the department and the Department of Law Enforcement of cybersecurity incidents.

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

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

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

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

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

Page 70 of 111

	576-02644-25 20257026
2031	public health or safety; national, state, or local security;
2032	economic security; civil liberties; or public confidence.
2033	(V) Level 1 is a low-level incident that is unlikely to
2034	impact public health or safety; national, state, or local
2035	security; economic security; civil liberties; or public
2036	confidence.
2037	b. The cybersecurity incident reporting process must
2038	specify the information that must be reported by a state agency
2039	following a cybersecurity incident or ransomware incident,
2040	which, at a minimum, must include the following:
2041	(I) A summary of the facts surrounding the cybersecurity
2042	incident or ransomware incident.
2043	(II) The date on which the state agency most recently
2044	backed up its data; the physical location of the backup, if the
2045	backup was affected; and if the backup was created using cloud
2046	computing.
2047	(III) The types of data compromised by the cybersecurity
2048	incident or ransomware incident.
2049	(IV) The estimated fiscal impact of the cybersecurity
2050	incident or ransomware incident.
2051	(V) In the case of a ransomware incident, the details of
2052	the ransom demanded.
2053	c.(I) A state agency shall report all ransomware incidents
2054	and any cybersecurity incident determined by the state agency to
2055	be of severity level 3, 4, or 5 to the state chief information
2056	security officer and the Cybercrime Office of the Department of
2057	Law Enforcement as soon as possible but no later than 48 hours
2058	after discovery of the cybersecurity incident and no later than
2059	12 hours after discovery of the ransomware incident. The report

Page 71 of 111

576-02644-2520257026_2060must contain the information required in sub-subparagraph b.2061(II) The state chief information security officer shall2062potify the President of the Senate and the Speaker of the House

notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 12 hours after receiving a state agency's incident report. The notification must include a high-level description of the incident and the likely effects.

2067 d. A state agency shall report a cybersecurity incident 2068 determined by the state agency to be of severity level 1 or 2 to 2069 the state chief information security officer and the Cybercrime 2070 Office of the Department of Law Enforcement as soon as possible, 2071 but no later than 96 hours after the discovery of the 2072 cybersecurity incident and no later than 72 hours after the 2073 discovery of the ransomware incident. The report must contain 2074 the information required in sub-subparagraph b.

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

81 <u>10.2.</u> Incorporating information obtained through detection 82 and response activities into the agency's cybersecurity incident 83 response plans.

84 <u>11.3.</u> Developing agency strategic and operational 85 cybersecurity plans required pursuant to this section.

2086 <u>12.4</u>. Establishing the managerial, operational, and 2087 technical safeguards for protecting state government data and 2088 information technology resources that align with the state

Page 72 of 111
2116

2117

```
576-02644-25
                                                              20257026
2089
      agency risk management strategy and that protect the
2090
      confidentiality, integrity, and availability of information and
2091
      data.
2092
           13. In coordination with the state chief information
2093
      technology procurement officer, establishing procedures for
2094
      procuring information technology commodities and services that
2095
      require the commodity or service to meet the National Institute
2096
      of Standards and Technology Cybersecurity Framework.
2097
           14.5. Submitting after-action reports following a
2098
      cybersecurity incident or ransomware incident. Such guidelines
2099
      and processes for submitting after-action reports must be
2100
      developed and published by July 1, 2027 December 1, 2022.
           (d) (c) Assist state agencies in complying with this
2101
      section.
2102
2103
           (e) (d) In collaboration with the Cybercrime Office of the
2104
      Department of Law Enforcement and through the state chief
2105
      information security officer and the Division of Enterprise
2106
      Information Technology Workforce Development, annually provide
2107
      training for state agency information security managers and
2108
      computer security incident response team members that contains
2109
      training on cybersecurity, including cybersecurity threats,
2110
      trends, and best practices.
2111
           (f) (e) Annually review the strategic and operational
2112
      cybersecurity plans of state agencies.
           (g) (f) Annually provide cybersecurity training through the
2113
      state chief information security officer and the Division of
2114
      Enterprise Information Technology Workforce Development to all
2115
```

Page 73 of 111

state agency technology professionals and employees with access

to highly sensitive information which develops, assesses, and

CODING: Words stricken are deletions; words underlined are additions.

SB 7026

576-02644-25 20257026 2118 documents competencies by role and skill level. The 2119 cybersecurity training curriculum must include training on the 2120 identification of each cybersecurity incident severity level referenced in sub-subparagraph (c)9.a. (b)1.a. The training may 2121 2122 be provided in collaboration with the Cybercrime Office of the 2123 Department of Law Enforcement, a private sector entity, or an 2124 institution of the State University System. 2125 (4) Each state agency head shall, at a minimum: (a) Designate an information security manager to administer 2126 2127 the cybersecurity program of the state agency. This designation 2128 must be provided annually in writing to ASSET the department by January 1. A state agency's information security manager, for 2129 2130 purposes of these information security duties, shall report 2131 directly to the agency head. 2132 (b) In consultation with the state chief information 2133 security officer department, through the Florida Digital 2134 Service, and the Cybercrime Office of the Department of Law 2135 Enforcement, establish an agency cybersecurity response team to 2136 respond to a cybersecurity incident. The agency cybersecurity 2137 response team shall convene upon notification of a cybersecurity incident and must immediately report all confirmed or suspected 2138 2139 incidents to the state chief information security officer, or 2140 his or her designee, and comply with all applicable guidelines 2141 and processes established pursuant to paragraph (3)(c) (3)(b). 2142 (C) Submit to state chief information security officer

annually by July 31 the state agency's strategic and operational cybersecurity plans developed pursuant to rules and guidelines established by the state chief information security officer.
1. The state agency strategic cybersecurity plan must cover

Page 74 of 111

CODING: Words stricken are deletions; words underlined are additions.

SB 7026

576-02644-25

20257026

2147 a 2-year period and, at a minimum, define security goals, 2148 intermediate objectives, and projected agency costs for the 2149 strategic issues of agency information security policy, risk management, security training, security incident response, and 2150 2151 disaster recovery. The plan must be based on the statewide 2152 cybersecurity strategic plan created by the state chief 2153 information security officer and include performance metrics 2154 that can be objectively measured to reflect the status of the state agency's progress in meeting security goals and objectives 2155 2156 identified in the agency's strategic information security plan.

2157 2. The state agency operational cybersecurity plan must 2158 include a set of measures that objectively assesses the 2159 performance of the agency's cybersecurity program in accordance 2160 with its risk management plan.

2161 (d) Conduct, and update every 2 years, a comprehensive risk 2162 assessment, which may be completed by a private sector vendor, 2163 to determine the security threats to the data, information, and 2164 information technology resources, including mobile devices and print environments, of the agency. The risk assessment must 2165 2166 comply with the risk assessment methodology developed by the 2167 state chief information security officer and is confidential and 2168 exempt from s. 119.07(1), except that such information shall be 2169 available to the Auditor General, the state chief information 2170 security officer, the Cybercrime Office of the Department of Law 2171 Enforcement, and, for state agencies under the jurisdiction of 2172 the Governor, the Chief Inspector General. If a private sector 2173 vendor is used to complete a comprehensive risk assessment, it 2174 must attest to the validity of the risk assessment findings. The 2175 comprehensive risk assessment must include all of the following:

Page 75 of 111

576-02644-25

2176 1. The results of vulnerability and penetration tests on 2177 any Internet website or mobile application that processes any 2178 sensitive personal information or confidential information and a 2179 plan to address any vulnerability identified in the tests. 2180 2. A written acknowledgment that the executive director or 2181 secretary of the agency, the chief financial officer of the 2182 agency, and each executive manager as designated by the state 2183 agency have been made aware of the risks revealed during the 2184 preparation of the agency's operational cybersecurity plan and 2185 the comprehensive risk assessment. 2186 (e) Develop, and periodically update, written internal policies and procedures, which include procedures for reporting 2187 2188 cybersecurity incidents and breaches to the Cybercrime Office of 2189 the Department of Law Enforcement and the state chief 2190 information security officer Florida Digital Service within the department. Such policies and procedures must be consistent with 2191 2192 the rules, guidelines, and processes established by ASSET the 2193 department to ensure the security of the data, information, and 2194 information technology resources of the agency. The internal 2195 policies and procedures that, if disclosed, could facilitate the 2196 unauthorized modification, disclosure, or destruction of data or 2197 information technology resources are confidential information 2198 and exempt from s. 119.07(1), except that such information shall 2199 be available to the Auditor General, the Cybercrime Office of 2200 the Department of Law Enforcement, the state chief information 2201 security officer the Florida Digital Service within the 2202 department, and, for state agencies under the jurisdiction of 2203 the Governor, the Chief Inspector General.

2204

(f) Implement managerial, operational, and technical

Page 76 of 111

CODING: Words stricken are deletions; words underlined are additions.

SB 7026

20257026

2205 safeguards and risk assessment remediation plans recommended by 2206 ASSET the department to address identified risks to the data, 2207 information, and information technology resources of the agency. 2208 The state chief information security officer department, through 2209 the Florida Digital Service, shall track implementation by state 2210 agencies upon development of such remediation plans in 2211 coordination with agency inspectors general. 2212 (g) Ensure that periodic internal audits and evaluations of 2213 the agency's cybersecurity program for the data, information, 2214 and information technology resources of the agency are 2215 conducted. The results of such audits and evaluations are confidential information and exempt from s. 119.07(1), except 2216 2217 that such information shall be available to the Auditor General, 2218 the Cybercrime Office of the Department of Law Enforcement, the 2219 state chief information security officer Florida Digital Service 2220 within the department, and, for agencies under the jurisdiction 2221 of the Governor, the Chief Inspector General. 2222 (h) Ensure that the cybersecurity requirements in the 2223 written specifications for the solicitation, contracts, and 2224 service-level agreement of information technology and 2225 information technology resources and services meet or exceed the 2226 applicable state and federal laws, regulations, and standards 2227 for cybersecurity, including the National Institute of Standards 2228 and Technology Cybersecurity Framework. Service-level agreements 2229 must identify service provider and state agency responsibilities 2230 for privacy and security, protection of government data, 2231 personnel background screening, and security deliverables with

576-02644-25

2232 2233 associated frequencies.

(i) Provide cybersecurity awareness training to all state

Page 77 of 111

CODING: Words stricken are deletions; words underlined are additions.

SB 7026

20257026

576-02644-25 20257026 2234 agency employees within 30 days after commencing employment, and 2235 annually thereafter, concerning cybersecurity risks and the 2236 responsibility of employees to comply with policies, standards, 2237 guidelines, and operating procedures adopted by the state agency 2238 to reduce those risks. The training may be provided in collaboration with the Cybercrime Office of the Department of 2239 2240 Law Enforcement, a private sector entity, or an institution of 2241 the State University System. 2242 (j) Develop a process for detecting, reporting, and 2243 responding to threats, breaches, or cybersecurity incidents 2244 which is consistent with the security rules, guidelines, and 2245 processes established by ASSET the department through the state 2246 chief information security officer Florida Digital Service. 2247 1. All cybersecurity incidents and ransomware incidents 2248 must be reported by state agencies. Such reports must comply 2249 with the notification procedures and reporting timeframes 2250 established pursuant to paragraph $(3)(c) \frac{(3)(b)}{(3)(c)}$. 2251 2. For cybersecurity breaches, state agencies shall provide 2252 notice in accordance with s. 501.171. 2253 (k) Submit to the state chief information security officer 2254 Florida Digital Service, within 1 week after the remediation of 2255 a cybersecurity incident or ransomware incident, an after-action 2256 report that summarizes the incident, the incident's resolution, 2257 and any insights gained as a result of the incident. 2258 The portions of records made confidential and exempt in (7) 2259 subsections (5) and (6) shall be available to the Auditor 2260 General, the Cybercrime Office of the Department of Law 2261 Enforcement, the state chief information security officer, the 2262 Legislature Florida Digital Service within the department, and,

Page 78 of 111

	576-02644-25 20257026
2263	for agencies under the jurisdiction of the Governor, the Chief
2264	Inspector General. Such portions of records may be made
2265	available to a local government, another state agency, or a
2266	federal agency for cybersecurity purposes or in furtherance of
2267	the state agency's official duties.
2268	(10) ASSET The department shall adopt rules relating to
2269	cybersecurity and to administer this section.
2270	Section 20. Section 282.3185, Florida Statutes, is amended
2271	to read:
2272	282.3185 Local government cybersecurity
2273	(1) SHORT TITLE.—This section may be cited as the "Local
2274	Government Cybersecurity Act."
2275	(2) DEFINITION.—As used in this section, the term "local
2276	government" means any county or municipality.
2277	(3) CYBERSECURITY TRAINING
2278	(a) The <u>state chief information security officer</u> Florida
2279	Digital Service shall:
2280	1. Develop a basic cybersecurity training curriculum for
2281	local government employees. All local government employees with
2282	access to the local government's network must complete the basic
2283	cybersecurity training within 30 days after commencing
2284	employment and annually thereafter.
2285	2. Develop an advanced cybersecurity training curriculum
2286	for local governments which is consistent with the cybersecurity
2287	training required under <u>s. 282.318(3)(f)</u>
2288	local government technology professionals and employees with
2289	access to highly sensitive information must complete the
2290	advanced cybersecurity training within 30 days after commencing
2291	employment and annually thereafter.

Page 79 of 111

CODING: Words stricken are deletions; words underlined are additions.

SB 7026

	576-02644-25 20257026
2292	(b) The <u>state chief information security officer</u> Florida
2293	Digital Service may provide the cybersecurity training required
2294	by this subsection in collaboration with the Cybercrime Office
2295	of the Department of Law Enforcement, a private sector entity,
2296	or an institution of the State University System.
2297	(4) CYBERSECURITY STANDARDS
2298	(a) Each local government shall adopt cybersecurity
2299	standards that safeguard its data, information technology, and
2300	information technology resources to ensure availability,
2301	confidentiality, and integrity. The cybersecurity standards must
2302	be consistent with generally accepted best practices for
2303	cybersecurity, including the National Institute of Standards and
2304	Technology Cybersecurity Framework.
2305	(b) Each county with a population of 75,000 or more must
2306	adopt the cybersecurity standards required by this subsection by
2307	January 1, 2024. Each county with a population of less than
2308	75,000 must adopt the cybersecurity standards required by this
2309	subsection by January 1, 2025.
2310	(c) Each municipality with a population of 25,000 or more
2311	must adopt the cybersecurity standards required by this
2312	subsection by January 1, 2024. Each municipality with a
2313	population of less than 25,000 must adopt the cybersecurity
2314	standards required by this subsection by January 1, 2025.
2315	(d) Each local government shall notify the <u>state chief</u>
2316	<u>information security officer</u> Florida Digital Service of its
2317	compliance with this subsection as soon as possible.
2318	(5) INCIDENT NOTIFICATION
2319	(a) A local government shall provide notification of a
2320	cybersecurity incident or ransomware incident to the <u>state chief</u>

Page 80 of 111

	576-02644-25 20257026
2321	
2322	the Cybercrime Office of the Department of Law Enforcement, and
2323	<u>the</u> sheriff who has jurisdiction over the local government in
2324	accordance with paragraph (b). The notification must include, at
2325	a minimum, the following information:
2326	1. A summary of the facts surrounding the cybersecurity
2327	incident or ransomware incident.
2328	2. The date on which the local government most recently
2329	backed up its data; the physical location of the backup, if the
2330	backup was affected; and if the backup was created using cloud
2331	computing.
2332	3. The types of data compromised by the cybersecurity
2333	incident or ransomware incident.
2334	4. The estimated fiscal impact of the cybersecurity
2335	incident or ransomware incident.
2336	5. In the case of a ransomware incident, the details of the
2337	ransom demanded.
2338	6. A statement requesting or declining assistance from the
2339	Cybersecurity Operations Center, the Cybercrime Office of the
2340	Department of Law Enforcement $_{m{ au}}$ or the sheriff who has
2341	jurisdiction over the local government.
2342	(b)1. A local government shall report all ransomware
2343	incidents and any cybersecurity incident determined by the local
2344	government to be of severity level 3, 4, or 5 as provided in <u>s.</u>
2345	282.318(3)(b) s. $282.318(3)(c)$ to the state chief information
2346	security officer Cybersecurity Operations Center , the Cybercrime
2347	Office of the Department of Law Enforcement, and the sheriff who
2348	has jurisdiction over the local government as soon as possible
2349	but no later than $\underline{12}$ $\underline{48}$ hours after discovery of the

Page 81 of 111

576-02644-25 20257026 2350 cybersecurity incident and no later than 6 12 hours after 2351 discovery of the ransomware incident. The report must contain 2352 the information required in paragraph (a). 2353 2. The state chief information security officer 2354 Cybersecurity Operations Center shall notify the state chief 2355 information officer, the Governor, the Commissioner of 2356 Agriculture, the Chief Financial Officer, the Attorney General, 2357 the President of the Senate, and the Speaker of the House of 2358 Representatives of any severity level 3, 4, or 5 incident as 2359 soon as possible but no later than 12 hours after receiving a local government's incident report. The notification must 2360 2361 include a high-level description of the incident and the likely 2362 effects. (c) A local government may report a cybersecurity incident 2363 2364 determined by the local government to be of severity level 1 or 2365 2 as provided in s. 282.318(3)(b) s. 282.318(3)(c) to the state 2366 chief information security officer Cybersecurity Operations 2367 Center, the Cybercrime Office of the Department of Law 2368 Enforcement, and the sheriff who has jurisdiction over the local 2369 government. The report shall contain the information required in 2370 paragraph (a). 2371 (d) The state chief information security officer 2372 Cybersecurity Operations Center shall provide a consolidated 2373 incident report by the 30th day after the end of each quarter on 2374 a quarterly basis to the Governor, the Commissioner of 2375 Agriculture, the Chief Financial Officer, the Attorney General, 2376 the President of the Senate, and the Speaker of the House of 2377 Representatives, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory 2378

Page 82 of 111

576-02644-25 20257026 2379 Council may not contain the name of any local government, 2380 network information, or system identifying information but must 2381 contain sufficient relevant information to allow the Florida 2382 Cybersecurity Advisory Council to fulfill its responsibilities 2383 as required in s. 282.319(9). 2384 (6) AFTER-ACTION REPORT.-A local government must submit to 2385 the state chief information security officer Florida Digital 2386 Service, within 1 week after the remediation of a cybersecurity 2387 incident or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any 2388 2389 insights gained as a result of the incident. By December 1, 2027 2390 2022, the state chief information security officer Florida 2391 Digital Service shall establish guidelines and processes for 2392 submitting an after-action report. 2393 Section 21. Effective July 1, 2026, paragraph (a) of 2394 subsection (3) and paragraphs (b) and (c) of subsection (5) of 2395 section 282.3185, Florida Statutes, as amended by this act, are 2396 amended to read: 2397 282.3185 Local government cybersecurity.-2398 (3) CYBERSECURITY TRAINING.-2399 (a) The state chief information security officer shall: 2400 1. Develop a basic cybersecurity training curriculum for 2401 local government employees. All local government employees with 2402 access to the local government's network must complete the basic cybersecurity training within 30 days after commencing 2403

2404 employment and annually thereafter.

2405 2. Develop an advanced cybersecurity training curriculum 2406 for local governments which is consistent with the cybersecurity 2407 training required under s. 282.318(3)(g) s. 282.318(3)(f). All

Page 83 of 111

576-02644-25 20257026 2408 local government technology professionals and employees with 2409 access to highly sensitive information must complete the 2410 advanced cybersecurity training within 30 days after commencing 2411 employment and annually thereafter. 2412 (5) INCIDENT NOTIFICATION.-2413 (b)1. A local government shall report all ransomware 2414 incidents and any cybersecurity incident determined by the local 2415 government to be of severity level 3, 4, or 5 as provided in s. 282.318(3)(c) s. 282.318(3)(b) to the state chief information 2416 2417 security officer, the Cybercrime Office of the Department of Law 2418 Enforcement, and the sheriff who has jurisdiction over the local 2419 government as soon as possible but no later than 12 hours after 2420 discovery of the cybersecurity incident and no later than 6 2421 hours after discovery of the ransomware incident. The report 2422 must contain the information required in paragraph (a). 2423 2. The state chief information security officer shall 2424 notify the state chief information officer, the Governor, the 2425 Commission of Agriculture, the Chief Financial Officer, the 2426 Attorney General, the President of the Senate and the Speaker of 2427 the House of Representatives of any severity level 3, 4, or 5 2428 incident as soon as possible but no later than 12 hours after

receiving a local government's incident report. The notification must include a high-level description of the incident and the likely effects.

(c) A local government may report a cybersecurity incident determined by the local government to be of severity level 1 or 2434 2 as provided in <u>s. 282.318(3)(c)</u> s. 282.318(3)(b) to the state chief information security officer, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has

Page 84 of 111

	576-02644-25 20257026
2437	jurisdiction over the local government. The report shall contain
2438	the information required in paragraph (a).
2439	Section 22. Section 282.319, Florida Statutes, is repealed.
2440	Section 23. (1) POSITIONS
2441	(a) The following positions are established within the
2442	Agency for State Systems and Enterprise Technology:
2443	1. Chief operations officer.
2444	2. Chief information officer.
2445	(b) Effective July 1, 2026, the following positions are
2446	established within the Agency for State Systems and Enterprise
2447	Technology, all of whom shall be appointed by the executive
2448	director:
2449	1. Deputy executive director, who shall serve as the state
2450	chief information architect, and the following:
2451	a. A minimum of six lead technology coordinators. At least
2452	one coordinator shall be assigned to each of the following major
2453	program areas: health and human services, education, government
2454	operations, criminal and civil justice, agriculture and natural
2455	resources, and transportation and economic development.
2456	b. A minimum of six assistant technology coordinators. At
2457	least one coordinator shall be assigned to each of the following
2458	major program areas: health and human services, education,
2459	government operations, criminal and civil justice, agriculture
2460	and natural resources, and transportation and economic
2461	development.
2462	2. State chief information security officer and six lead
2463	security consultants. One consultant shall be assigned to each
2464	of the following major program areas: health and human services,
2465	education, government operations, criminal and civil justice,

Page 85 of 111

	576-02644-25 20257026
2466	agriculture and natural resources, and transportation and
2467	economic development.
2468	3. State chief data officer and the following:
2469	a. A minimum of three data specialists with at least one
2470	specialist dedicated to each of the following areas of data
2471	expertise:
2472	(I) Personally identifiable information.
2473	(II) Protected health information.
2474	(III) Criminal justice information services.
2475	b. A minimum of six data security consultants. At least one
2476	consultant shall be assigned to each of the following major
2477	program areas: health and human services, education, government
2478	operations, criminal and civil justice, agriculture and natural
2479	resources, and transportation and economic development.
2480	4. State chief information technology procurement officer
2481	and a minimum of six lead information technology procurement
2482	consultants. At least one coordinator shall be assigned to each
2483	of the following major program areas: health and human services,
2484	education, government operations, criminal and civil justice,
2485	agriculture and natural resources, and transportation and
2486	economic development.
2487	5. State chief technology officer and the following:
2488	a. A minimum of 42 information technology business analyst
2489	consultants that shall be assigned to major program areas as
2490	follows:
2491	(I) At least 11 consultants shall be assigned to health and
2492	human services and dedicated to state agencies at a minimum as
2493	follows:
2494	(A) Two dedicated to the Department of Health.
I	

Page 86 of 111

	576-02644-25 20257026
2495	(B) Four dedicated to the Agency for Health Care
2496	Administration.
2497	(C) Three dedicated to the Department of Children and
2498	Families.
2499	(D) Two dedicated to the remaining health and human
2500	services state agencies.
2501	(II) At least four consultants shall be assigned to
2502	education.
2503	(III) At least eight consultants shall be assigned to
2504	government operations and dedicated to state agencies at a
2505	minimum as follows:
2506	(A) Two dedicated to the Department of Financial Services.
2507	(B) One dedicated to the Department of Business and
2508	Professional Regulation.
2509	(C) Two dedicated to the Department of Management Services.
2510	(D) Three dedicated to the remaining government operations
2511	state agencies.
2512	(IV) At least six consultants shall be assigned to criminal
2513	and civil justice and dedicated to state agencies at a minimum
2514	as follows:
2515	(A) One dedicated to the Department of Law Enforcement.
2516	(B) Two dedicated to the Department of Corrections.
2517	(C) One dedicated to the Department of Juvenile Justice.
2518	(D) One dedicated to the Department of Legal Affairs.
2519	(E) One dedicated to the remaining criminal and civil
2520	justice state agencies.
2521	(V) At least four consultants shall be assigned to
2522	agriculture and natural resources and dedicated to state
2523	agencies at a minimum as follows:

Page 87 of 111

	576-02644-25 20257026
2524	(A) One dedicated the Department of Agriculture and
2525	Consumer Services.
2526	(B) One dedicated to the Department of Environmental
2527	Protection.
2528	(C) One dedicated to the Fish and Wildlife Conservation
2529	Commission.
2530	(D) One dedicated to the remaining agriculture and natural
2531	resources state agencies.
2532	(VI) At least nine consultants shall be assigned to
2533	transportation and economic development and dedicated to state
2534	agencies at a minimum as follows:
2535	(A) Two dedicated to the Department of Transportation.
2536	(B) Two dedicated to the Department of State.
2537	(C) One dedicated to the Department of Highway Safety and
2538	Motor Vehicles.
2539	(D) Two dedicated to the Department of Commerce.
2540	(E) One dedicated to the Division of Emergency Management.
2541	(F) One dedicated to the remaining transportation and
2542	economic development state agencies.
2543	b. A minimum of six information technology project
2544	management professional consultants. At least one consultant
2545	shall be assigned to each of the following major program areas:
2546	health and human services, education, government operations,
2547	criminal and civil justice, agriculture and natural resources,
2548	and transportation and economic development.
2549	c. A minimum of six information technology contract
2550	management consultants. At least one consultant shall be
2551	assigned to each of the following major program areas: health
2552	and human services, education, government operations, criminal

Page 88 of 111

	576-02644-25 20257026
2553	and civil justice, agriculture and natural resources, and
2554	transportation and economic development.
2555	d. A minimum of six information technology quality
2556	assurance consultants. At least one consultant shall be assigned
2557	to each of the following major program areas: health and human
2558	services, education, government operations, criminal and civil
2559	justice, agriculture and natural resources, and transportation
2560	and economic development.
2561	6. State chief of information technology workforce
2562	development.
2563	(2) BUREAUS.—
2564	(a) The Division of Enterprise Information Technology
2565	Services shall include:
2566	1. The Bureau of Enterprise Information Technology
2567	Operations, responsible for assessing state agency information
2568	technology needs and risks as established under s. 282.006,
2569	Florida Statutes.
2570	2. The Bureau of Enterprise Information Technology Quality
2571	Assurance, responsible for activities established under s.
2572	282.006, Florida Statutes.
2573	3. The Bureau of Enterprise Information Technology Project
2574	Management, responsible for project management oversight and
2575	activities established under s. 282.006, Florida Statutes.
2576	4. The Bureau of Enterprise Information Technology Contract
2577	Management, responsible for contract management oversight and
2578	activities established under s. 282.006, Florida Statutes.
2579	(b) The Division of Enterprise Information Technology
2580	Purchasing shall include:
2581	1. The Bureau of Enterprise Information Technology

Page 89 of 111

	576-02644-25 20257026
2582	Procurement Services, responsible for procurement activities
2583	established under s. 282.006, Florida Statutes.
2584	2. The Bureau of Enterprise Information Technology
2585	Procurement Policy and Oversight, responsible for activities
2586	established under s. 282.006, Florida Statutes.
2587	(3) WORKGROUP
2588	(a) The chief information officer policy workgroup shall be
2589	composed of all state agency chief information officers.
2590	(b) The purpose of the workgroup is to provide the
2591	Legislature with input and feedback regarding the structure,
2592	budget, and governance of the Agency for State Systems and
2593	Enterprise Technology.
2594	(c) The chair of the workgroup shall be the interim state
2595	chief information officer.
2596	(d) The voting members of the workgroup shall include the
2597	chair of the workgroup and the chief information officers from
2598	the Department of Financial Services, the Department of
2599	Agriculture and Consumer Services, and the Department of Legal
2600	Affairs.
2601	(e) The chair of the workgroup shall submit a report to the
2602	Governor, the Commissioner of Agriculture, the Chief Financial
2603	Officer, the Attorney General, the President of the Senate, and
2604	the Speaker of the House of Representatives which includes
2605	recommendations and justifications for changes by December 1,
2606	2025. The final report must be voted on and accepted by a
2607	unanimous vote of the voting members of the workgroup.
2608	(f) The workgroup shall expire after submission of the
2609	report required in paragraph (e).
2610	Section 24. Section 282.201, Florida Statutes, is amended
1	

Page 90 of 111

	576-02644-25 20257026
2611	to read:
2612	282.201 State data centerThe state data center is
2613	established within the Northwest Regional Data Center pursuant
2614	to s. 282.0211 and shall meet or exceed the information
2615	technology standards specified in ss. 282.006 and 282.318 the
2616	department. The provision of data center services must comply
2617	with applicable state and federal laws, regulations, and
2618	policies, including all applicable security, privacy, and
2619	auditing requirements. The department shall appoint a director
2620	of the state data center who has experience in leading data
2621	center facilities and has expertise in cloud-computing
2622	management.
2623	(1) STATE DATA CENTER DUTIESThe state data center shall:
2624	(a)—Offer, develop, and support the services and
2625	applications defined in service-level agreements executed with
2626	its customer entities.
2627	(b) Maintain performance of the state data center by
2628	ensuring proper data backup; data backup recovery; disaster
2629	recovery; and appropriate security, power, cooling, fire
2630	suppression, and capacity.
2631	(c) Develop and implement business continuity and disaster
2632	recovery plans, and annually conduct a live exercise of each
2633	plan.
2634	(d) Enter into a service-level agreement with each customer
2635	entity to provide the required type and level of service or
2636	services. If a customer entity fails to execute an agreement
2637	within 60 days after commencement of a service, the state data
2638	center may cease service. A service-level agreement may not have
2639	a term exceeding 3 years and at a minimum must:
I	

Page 91 of 111

	576-02644-25 20257026
2640	1. Identify the parties and their roles, duties, and
2641	responsibilities under the agreement.
2642	2. State the duration of the contract term and specify the
2643	conditions for renewal.
2644	3. Identify the scope of work.
2645	4. Identify the products or services to be delivered with
2646	sufficient specificity to permit an external financial or
2647	performance audit.
2648	5. Establish the services to be provided, the business
2649	standards that must be met for each service, the cost of each
2650	service by agency application, and the metrics and processes by
2651	which the business standards for each service are to be
2652	objectively measured and reported.
2653	6. Provide a timely billing methodology to recover the
2654	costs of services provided to the customer entity pursuant to s.
2655	215.422.
2656	7.—Provide a procedure for modifying the service-level
2657	agreement based on changes in the type, level, and cost of a
2658	service.
2659	8.—Include a right-to-audit clause to ensure that the
2660	parties to the agreement have access to records for audit
2661	purposes during the term of the service-level agreement.
2662	9.—Provide that a service-level agreement may be terminated
2663	by either party for cause only after giving the other party and
2664	the department notice in writing of the cause for termination
2665	and an opportunity for the other party to resolve the identified
2666	cause within a reasonable period.
2667	10. Provide for mediation of disputes by the Division of
2668	Administrative Hearings pursuant to s. 120.573.

Page 92 of 111

	576-02644-25 20257026
2669	(e)—For purposes of chapter 273, be the custodian of
2670	resources and equipment located in and operated, supported, and
2671	managed by the state data center.
2672	(f) Assume administrative access rights to resources and
2673	equipment, including servers, network components, and other
2674	devices, consolidated into the state data center.
2675	1. Upon consolidation, a state agency shall relinquish
2676	administrative rights to consolidated resources and equipment.
2677	State agencies required to comply with federal and state
2678	criminal justice information security rules and policies shall
2679	retain administrative access rights sufficient to comply with
2680	the management control provisions of those rules and policies;
2681	however, the state data center shall have the appropriate type
2682	or level of rights to allow the center to comply with its duties
2683	pursuant to this section. The Department of Law Enforcement
2684	shall serve as the arbiter of disputes pertaining to the
2685	appropriate type and level of administrative access rights
2686	pertaining to the provision of management control in accordance
2687	with the federal criminal justice information guidelines.
2688	2. The state data center shall provide customer entities
2689	with access to applications, servers, network components, and
2690	other devices necessary for entities to perform business
2691	activities and functions, and as defined and documented in a
2692	service-level agreement.
2693	(g) In its procurement process, show preference for cloud-
2694	computing solutions that minimize or do not require the
2695	purchasing, financing, or leasing of state data center
2696	infrastructure, and that meet the needs of customer agencies,
2697	that reduce costs, and that meet or exceed the applicable state

Page 93 of 111

2726

I	576-02644-25 20257026
2698	and federal laws, regulations, and standards for cybersecurity.
2699	(h) Assist customer entities in transitioning from state
2700	data center services to the Northwest Regional Data Center or
2701	other third-party cloud-computing services procured by a
2702	customer entity or by the Northwest Regional Data Center on
2703	behalf of a customer entity.
2704	(1) (2) USE OF THE STATE DATA CENTER
2705	(a) The following are exempt from the use of the state data
2706	center: the Department of Law Enforcement, the Department of the
2707	Lottery's Gaming System, Systems Design and Development in the
2708	Office of Policy and Budget, the regional traffic management
2709	centers as described in s. 335.14(2) and the Office of Toll
2710	Operations of the Department of Transportation, the State Board
2711	of Administration, state attorneys, public defenders, criminal
2712	conflict and civil regional counsel, capital collateral regional
2713	counsel, and the Florida Housing Finance Corporation <u>, and the</u>
2714	Division of Emergency Management within the Executive Office of
2715	the Governor.
2716	(b) The Division of Emergency Management is exempt from the
2717	use of the state data center. This paragraph expires July 1,
2718	2025.
2719	(2)(3) AGENCY LIMITATIONSUnless exempt from the use of
2720	the state data center pursuant to this section or authorized by
2721	the Legislature, a state agency may not:
2722	(a) Create a new agency computing facility or data center,
2723	or expand the capability to support additional computer
2724	equipment in an existing agency computing facility or data
2725	center; or

(b) Terminate services with the state data center without

Page 94 of 111

	576-02644-25 20257026
2727	giving written notice of intent to terminate services 180 days
2728	before such termination.
2729	(4) DEPARTMENT RESPONSIBILITIES.—The department shall
2730	provide operational management and oversight of the state data
2731	center, which includes:
2732	(a) Implementing industry standards and best practices for
2733	the state data center's facilities, operations, maintenance,
2734	planning, and management processes.
2735	(b) Developing and implementing cost-recovery mechanisms
2736	that recover the full direct and indirect cost of services
2737	through charges to applicable customer entities. Such cost-
2738	recovery mechanisms must comply with applicable state and
2739	federal regulations concerning distribution and use of funds and
2740	must ensure that, for any fiscal year, no service or customer
2741	entity subsidizes another service or customer entity. The
2742	department may recommend other payment mechanisms to the
2743	Executive Office of the Governor, the President of the Senate,
2744	and the Speaker of the House of Representatives. Such mechanisms
2745	may be implemented only if specifically authorized by the
2746	Legislature.
2747	(c) Developing and implementing appropriate operating
2748	guidelines and procedures necessary for the state data center to
2749	perform its duties pursuant to subsection (1). The guidelines
2750	and procedures must comply with applicable state and federal
2751	laws, regulations, and policies and conform to generally
2752	accepted governmental accounting and auditing standards. The
2753	guidelines and procedures must include, but need not be limited
2754	to:
2755	1. Implementing a consolidated administrative support

Page 95 of 111

0756	576-02644-25 20257026
2756	structure responsible for providing financial management,
2757	procurement, transactions involving real or personal property,
2758	human resources, and operational support.
2759	2. Implementing an annual reconciliation process to ensure
2760	that each customer entity is paying for the full direct and
2761	indirect cost of each service as determined by the customer
2762	entity's use of each service.
2763	3. Providing rebates that may be credited against future
2764	billings to customer entities when revenues exceed costs.
2765	4. Requiring customer entities to validate that sufficient
2766	funds exist before implementation of a customer entity's request
2767	for a change in the type or level of service provided, if such
2768	change results in a net increase to the customer entity's cost
2769	for that fiscal year.
2770	5. By November 15 of each year, providing to the Office of
2771	Policy and Budget in the Executive Office of the Covernor and to
2772	the chairs of the legislative appropriations committees the
2773	projected costs of providing data center services for the
2774	following fiscal year.
2775	6. Providing a plan for consideration by the Legislative
2776	Budget Commission if the cost of a service is increased for a
2777	reason other than a customer entity's request made pursuant to
2778	subparagraph 4. Such a plan is required only if the service cost
2779	increase results in a net increase to a customer entity for that
2780	fiscal year.
2781	7. Standardizing and consolidating procurement and
2782	contracting practices.
2783	(d) In collaboration with the Department of Law Enforcement
2784	and the Florida Digital Service, developing and implementing a
	Page 96 of 111

	576-02644-25 20257026
2785	 process for detecting, reporting, and responding to
2786	cybersecurity incidents, breaches, and threats.
2787	(c) Adopting rules relating to the operation of the state
2788	data center, including, but not limited to, budgeting and
2789	accounting procedures, cost-recovery methodologies, and
2790	operating procedures.
2791	(5) NORTHWEST REGIONAL DATA CENTER CONTRACTIn order for
2792	the department to carry out its duties and responsibilities
2793	relating to the state data center, the secretary of the
2794	department shall contract by July 1, 2022, with the Northwest
2795	Regional Data Center pursuant to s. 287.057(11). The contract
2796	shall provide that the Northwest Regional Data Center will
2797	manage the operations of the state data center and provide data
2798	center services to state agencies.
2799	(a) The department shall provide contract oversight,
2800	including, but not limited to, reviewing invoices provided by
2801	the Northwest Regional Data Center for services provided to
2802	state agency customers.
2803	(b) The department shall approve or request updates to
2804	invoices within 10 business days after receipt. If the
2805	department does not respond to the Northwest Regional Data
2806	Center, the invoice will be approved by default. The Northwest
2807	Regional Data Center must submit approved invoices directly to
2808	state agency customers.
2809	Section 25. Section 282.0211, Florida Statutes, is created
2810	to read:
2811	282.0211 Northwest Regional Data Center
2812	(1) For the purpose of providing data center services to
2813	its state agency customers, the Northwest Regional Data Center
·	Page 97 of 111

Page 97 of 111

	576-02644-25 20257026
2814	is designated as the state data center for all state agencies
2815	and shall:
2816	(a) Operate under a governance structure that represents
2817	its customers proportionally.
2818	(b) Maintain an appropriate cost-allocation methodology
2819	that accurately bills state agency customers based solely on the
2820	actual direct and indirect costs of the services provided to
2821	state agency customers and ensures that, for any fiscal year,
2822	state agency customers are not subsidizing other customers of
2823	the data center. Such cost-allocation methodology must comply
2824	with applicable state and federal regulations concerning the
2825	distribution and use of state and federal funds.
2826	(c) Enter into a service-level agreement with each state
2827	agency customer to provide services as defined and approved by
2828	the governing board of the center. At a minimum, such service-
2829	level agreements must:
2830	1. Identify the parties and their roles, duties, and
2831	responsibilities under the agreement;
2832	2. State the duration of the agreement term, which may not
2833	exceed 3 years, and specify the conditions for up to two
2834	optional 1-year renewals of the agreement before execution of a
2835	new agreement;
2836	3. Identify the scope of work;
2837	4. Establish the services to be provided, the business
2838	standards that must be met for each service, the cost of each
2839	service, and the process by which the business standards for
2840	each service are to be objectively measured and reported;
2841	5. Provide a timely billing methodology for recovering the
2842	cost of services provided pursuant to s. 215.422;

Page 98 of 111

	576-02644-25 20257026
2843	6. Provide a procedure for modifying the service-level
2844	agreement to address any changes in projected costs of service;
2845	7. Include a right-to-audit clause to ensure that the
2846	parties to the agreement have access to records for audit
2847	purposes during the term of the service-level agreement;
2848	8. Identify the products or services to be delivered with
2849	sufficient specificity to permit an external financial or
2850	performance audit;
2851	9. Provide that the service-level agreement may be
2852	terminated by either party for cause only after giving the other
2853	party notice in writing of the cause for termination and an
2854	opportunity for the other party to resolve the identified cause
2855	within a reasonable period; and
2856	10. Provide state agency customer entities with access to
2857	applications, servers, network components, and other devices
2858	necessary for entities to perform business activities and
2859	functions and as defined and documented in a service-level
2860	agreement.
2861	(d) In its procurement process, show preference for cloud-
2862	computing solutions that minimize or do not require the
2863	purchasing or financing of state data center infrastructure,
2864	that meet the needs of state agency customer entities, that
2865	reduce costs, and that meet or exceed the applicable state and
2866	federal laws, regulations, and standards for cybersecurity.
2867	(e) Assist state agency customer entities in transitioning
2868	from state data center services to other third-party cloud-
2869	computing services procured by a customer entity or by the
2870	Northwest Regional Data Center on behalf of the customer entity.
2871	(f) Provide to the Board of Governors the total annual

Page 99 of 111

	576-02644-25 20257026
2872	budget by major expenditure category, including, but not limited
2873	to, salaries, expenses, operating capital outlay, contracted
2874	services, or other personnel services, by July 30 each fiscal
2875	year.
2876	(g) Provide to each state agency customer its projected
2877	annual cost for providing the agreed-upon data center services
2878	by September 1 each fiscal year.
2879	(h) By November 15 of each year, provide to the Office of
2880	Policy and Budget in the Executive Office of the Governor and to
2881	the chairs of the legislative appropriations committees the
2882	projected costs of providing data center services for the
2883	following fiscal year.
2884	(i) Provide a plan for consideration by the Legislative
2885	Budget Commission if the governing body of the center approves
2886	the use of a billing rate schedule after the start of the fiscal
2887	year that increases any state agency customer's costs for that
2888	fiscal year.
2889	(j) Provide data center services that comply with
2890	applicable state and federal laws, regulations, and policies,
2891	including all applicable security, privacy, and auditing
2892	requirements.
2893	(k) Maintain performance of the data center facilities by
2894	ensuring proper data backup; data backup recovery; disaster
2895	recovery; and appropriate security, power, cooling, fire
2896	suppression, and capacity.
2897	(1) Submit invoices to state agency customers.
2898	(m) As funded in the General Appropriations Act, provide
2899	data center services to state agencies from multiple facilities.
2900	(2) Unless exempt from the requirement to use the state
I	

Page 100 of 111

CODING: Words stricken are deletions; words underlined are additions.

SB 7026

	576-02644-25 20257026
2901	data center pursuant to s. 282.201(1) or as authorized by the
2902	Legislature, a state agency may not do any of the following:
2903	(a) Terminate services with the Northwest Regional Data
2904	Center without giving written notice of intent to terminate
2905	services 180 days before such termination.
2906	(b) Procure third-party cloud-computing services without
2907	evaluating the cloud-computing services provided by the
2908	Northwest Regional Data Center.
2909	(c) Exceed 30 days from receipt of approved invoices to
2910	remit payment for state data center services provided by the
2911	Northwest Regional Data Center.
2912	(3) The Northwest Regional Data Center's authority to
2913	provide data center services to its state agency customers may
2914	be terminated if:
2915	(a) The center requests such termination to the Board of
2916	Governors, the President of the Senate, and the Speaker of the
2917	House of Representatives; or
2918	(b) The center fails to comply with the provisions of this
2919	section.
2920	(4) If such authority is terminated, the center has 1 year
2921	to provide for the transition of its state agency customers to a
2922	qualified alternative cloud-based data center that meets the
2923	enterprise architecture standards established pursuant to this
2924	chapter.
2925	Section 26. Section 1004.649, Florida Statutes, is amended
2926	to read:
2927	1004.649 Northwest Regional Data CenterThere is created
2928	at Florida State University the Northwest Regional Data Center.
2929	The data center shall serve as the state data center as
I	

Page 101 of 111

	576-02644-25 20257026
2930	designated in s. 282.201
2931	(1) For the purpose of providing data center services to
2932	its state agency customers, the Northwest Regional Data Center
2933	is designated as a state data center for all state agencies and
2934	shall:
2935	(a) Operate under a governance structure that represents
2936	its customers proportionally.
2937	(b) Maintain an appropriate cost-allocation methodology
2938	that accurately bills state agency customers based solely on the
2939	actual direct and indirect costs of the services provided to
2940	state agency customers and ensures that, for any fiscal year,
2941	state agency customers are not subsidizing other customers of
2942	the data center. Such cost-allocation methodology must comply
2943	with applicable state and federal regulations concerning the
2944	distribution and use of state and federal funds.
2945	(c) Enter into a service-level agreement with each state
2946	agency customer to provide services as defined and approved by
2947	the governing board of the center. At a minimum, such service-
2948	level agreements must:
2949	1. Identify the parties and their roles, duties, and
2950	responsibilities under the agreement;
2951	2. State the duration of the agreement term, which may not
2952	exceed 3 years, and specify the conditions for up to two
2953	optional 1-year renewals of the agreement before execution of a
2954	new agreement;
2955	3Identify the scope of work;
2956	4. Establish the services to be provided, the business
2957	standards that must be met for each service, the cost of each
2958	service, and the process by which the business standards for

Page 102 of 111

576-02644-25 20257026 2959 each service are to be objectively measured and reported; 2960 5. Provide a timely billing methodology for recovering the 2961 cost of services provided pursuant to s. 215.422; 2962 6. Provide a procedure for modifying the service-level 2963 agreement to address any changes in projected costs of service; 2964 7. Include a right-to-audit clause to ensure that the 2965 parties to the agreement have access to records for audit 2966 purposes during the term of the service-level agreement; Identify the products or services to be delivered with 2967 2968 sufficient specificity to permit an external financial or 2969 performance audit; 2970 9. Provide that the service-level agreement may be 2971 terminated by either party for cause only after giving the other 2972 party notice in writing of the cause for termination and an 2973 opportunity for the other party to resolve the identified cause 2974 within a reasonable period; and 2975 10. Provide state agency customer entities with access to 2976 applications, servers, network components, and other devices 2977 necessary for entities to perform business activities and 2978 functions and as defined and documented in a service-level 2979 agreement. 2980 (d) In its procurement process, show preference for cloud-2981 computing solutions that minimize or do not require the 2982 purchasing or financing of state data center infrastructure, 2983 that meet the needs of state agency customer entities, that 2984 reduce costs, and that meet or exceed the applicable state and 2985 federal laws, regulations, and standards for cybersecurity. 2986 (c) Assist state agency customer entities in transitioning 2987 from state data center services to other third-party cloud-

Page 103 of 111

	576-02644-25 20257026
2988	computing services procured by a customer entity or by the
2989	Northwest Regional Data Center on behalf of the customer entity.
2990	(f) Provide to the Board of Governors the total annual
2991	budget by major expenditure category, including, but not limited
2992	to, salaries, expenses, operating capital outlay, contracted
2993	services, or other personnel services by July 30 each fiscal
2994	year.
2995	(g) Provide to each state agency customer its projected
2996	annual cost for providing the agreed-upon data center services
2997	by September 1 each fiscal year.
2998	(h) Provide a plan for consideration by the Legislative
2999	Budget Commission if the governing body of the center approves
3000	the use of a billing rate schedule after the start of the fiscal
3001	year that increases any state agency customer's costs for that
3002	fiscal year.
3003	(i) Provide data center services that comply with
3004	applicable state and federal laws, regulations, and policies,
3005	including all applicable security, privacy, and auditing
3006	requirements.
3007	(j) Maintain performance of the data center facilities by
3008	ensuring proper data backup; data backup recovery; disaster
3009	recovery; and appropriate security, power, cooling, fire
3010	suppression, and capacity.
3011	(k) Prepare and submit state agency customer invoices to
3012	the Department of Management Services for approval. Upon
3013	approval or by default pursuant to s. 282.201(5), submit
3014	invoices to state agency customers.
3015	(1) As funded in the General Appropriations Act, provide
3016	data center services to state agencies from multiple facilities.
ļ	
	Page 104 of 111

	576-02644-25 20257026
3017	(2) Unless exempt from the requirement to use the state
3018	data center pursuant to s. 282.201(2) or as authorized by the
3019	Legislature, a state agency may not do any of the following:
3020	(a) Terminate services with the Northwest Regional Data
3021	Center without giving written notice of intent to terminate
3022	services 180 days before such termination.
3023	(b) Procure third-party cloud-computing services without
3024	evaluating the cloud-computing services provided by the
3025	Northwest Regional Data Center.
3026	(c) Exceed 30 days from receipt of approved invoices to
3027	remit payment for state data center services provided by the
3028	Northwest Regional Data Center.
3029	(3) The Northwest Regional Data Center's authority to
3030	provide data center services to its state agency customers may
3031	be terminated if:
3032	(a) The center requests such termination to the Board of
3033	Governors, the President of the Senate, and the Speaker of the
3034	House of Representatives; or
3035	(b) The center fails to comply with the provisions of this
3036	section.
3037	(4) If such authority is terminated, the center has 1 year
3038	to provide for the transition of its state agency customers to a
3039	qualified alternative cloud-based data center that meets the
3040	enterprise architecture standards established by the Florida
3041	Digital Service.
3042	Section 27. Effective July 1, 2026, subsection (2) of
3043	section 20.22, Florida Statutes, is amended to read:
3044	20.22 Department of Management ServicesThere is created a
3045	Department of Management Services.
	Page 105 of 111

	576-02644-25 20257026
3046	(2) The following divisions, programs, and services within
3047	the Department of Management Services are established:
3048	(a) Facilities Program.
3049	(b) The Florida Digital Service.
3050	(c) Workforce Program.
3051	<u>(c)1.</u> (d)1. Support Program.
3052	2. Federal Property Assistance Program.
3053	<u>(d)</u> Administration Program.
3054	<u>(e)</u> Division of Administrative Hearings.
3055	<u>(f)</u> Division of Retirement.
3056	<u>(g)</u> (h) Division of State Group Insurance.
3057	(h)(i) Division of Telecommunications.
3058	Section 28. Effective July 1, 2026, subsections (1), (5),
3059	(7), and (8) of section 282.802, Florida Statutes, are amended
3060	to read:
3061	282.802 Government Technology Modernization Council
3062	(1) The Government Technology Modernization Council, an
3063	advisory council as defined in s. 20.03(7), is <u>located</u> created
3064	within <u>ASSET</u> the department. Except as otherwise provided in
3065	this section, the advisory council shall operate in a manner
3066	consistent with s. 20.052.
3067	(5) The state chief information officer Secretary of
3068	Management Services, or his or her designee, shall serve as the
3069	ex officio, nonvoting executive director of the council.
3070	(7) (a) The council shall meet at least quarterly to:
3071	(a) 1. Recommend legislative and administrative actions that
3072	the Legislature and state agencies as defined in <u>s. 282.0041</u> s.
3073	282.318(2) may take to promote the development of data
3074	modernization in this state.

Page 106 of 111

	576-02644-25 20257026
3075	
3076	reforms and the creation of a state code of ethics for
3077	artificial intelligence systems in state government.
3078	(c) 3. Assess the effect of automated decision systems or
3079	identity management on constitutional and other legal rights,
3080	duties, and privileges of residents of this state.
3081	(d)4. Evaluate common standards for artificial intelligence
3082	safety and security measures, including the benefits of
3083	requiring disclosure of the digital provenance for all images
3084	and audio created using generative artificial intelligence as a
3085	means of revealing the origin and edit of the image or audio, as
3086	well as the best methods for such disclosure.
3087	<u>(e)</u> 5. Assess the manner in which governmental entities and
3088	the private sector are using artificial intelligence with a
3089	focus on opportunity areas for deployments in systems across
3090	this state.
3091	(f) 6. Determine the manner in which artificial intelligence
3092	is being exploited by bad actors, including foreign countries of
3093	concern as defined in s. 287.138(1).
3094	<u>(g)</u> 7. Evaluate the need for curriculum to prepare school-
3095	age audiences with the digital media and visual literacy skills
3096	needed to navigate the digital information landscape.
3097	(b) At least one quarterly meeting of the council must be a
3098	joint meeting with the Florida Cybersecurity Advisory Council.
3099	(8) By December 31, 2024, and Each December 31 thereafter,
3100	the council shall submit to the Governor, <u>the Commissioner of</u>
3101	Agriculture, the Chief Financial Officer, the Attorney General,
3102	the President of the Senate, and the Speaker of the House of
3103	Representatives any legislative recommendations considered

Page 107 of 111

CODING: Words stricken are deletions; words underlined are additions.

SB 7026

```
576-02644-25
                                                              20257026
3104
      necessary by the council to modernize government technology,
3105
      including:
            (a) Recommendations for policies necessary to:
3106
3107
           1. Accelerate adoption of technologies that will increase
3108
      productivity of state enterprise information technology systems,
3109
      improve customer service levels of government, and reduce
3110
      administrative or operating costs.
3111
           2. Promote the development and deployment of artificial
      intelligence systems, financial technology, education
3112
3113
      technology, or other enterprise management software in this
3114
      state.
           3. Protect Floridians from bad actors who use artificial
3115
3116
      intelligence.
            (b) Any other information the council considers relevant.
3117
3118
           Section 29. Effective July 1, 2026, section 282.604,
3119
      Florida Statutes, is amended to read:
3120
           282.604 Adoption of rules.-ASSET The Department of
3121
      Management Services shall, with input from stakeholders, adopt
3122
      rules pursuant to ss. 120.536(1) and 120.54 for the development,
3123
      procurement, maintenance, and use of accessible electronic
3124
      information technology by governmental units.
3125
           Section 30. Subsection (4) of section 287.0591, Florida
3126
      Statutes, is amended to read:
3127
           287.0591 Information technology; vendor disqualification.-
3128
            (4) If the department issues a competitive solicitation for
3129
      information technology commodities, consultant services, or
3130
      staff augmentation contractual services, the state chief
3131
      information officer must Florida Digital Service within the
3132
      department shall participate in such solicitations.
```

Page 108 of 111

576-02644-25 20257026_ 3133 Section 31. Subsection (4) of section 288.012, Florida 3134 Statutes, is amended to read: 3135 288.012 State of Florida international offices; direct-

3136 support organization.-The Legislature finds that the expansion 3137 of international trade and tourism is vital to the overall 3138 health and growth of the economy of this state. This expansion 3139 is hampered by the lack of technical and business assistance, 3140 financial assistance, and information services for businesses in this state. The Legislature finds that these businesses could be 3141 3142 assisted by providing these services at State of Florida 3143 international offices. The Legislature further finds that the 3144 accessibility and provision of services at these offices can be 3145 enhanced through cooperative agreements or strategic alliances 3146 between private businesses and state, local, and international 3147 governmental entities.

3148 (4) The Department of Commerce, in connection with the 3149 establishment, operation, and management of any of its offices 3150 located in another country, is exempt from the provisions of ss. 3151 255.21, 255.25, and 255.254 relating to leasing of buildings; 3152 ss. 283.33 and 283.35 relating to bids for printing; ss. 3153 287.001-287.20 relating to purchasing and motor vehicles; and 3154 ss. 282.0051 and 282.702-282.7101 ss. 282.003-282.00515 and 3155 282.702-282.7101 relating to communications, and from all 3156 statutory provisions relating to state employment.

3157 (a) The department may exercise such exemptions only upon3158 prior approval of the Governor.

(b) If approval for an exemption under this section is granted as an integral part of a plan of operation for a specified international office, such action shall constitute

Page 109 of 111

1	576-02644-25 20257026
3162	continuing authority for the department to exercise the
3163	exemption, but only in the context and upon the terms originally
3164	granted. Any modification of the approved plan of operation with
3165	respect to an exemption contained therein must be resubmitted to
3166	the Governor for his or her approval. An approval granted to
3167	exercise an exemption in any other context shall be restricted
3168	to the specific instance for which the exemption is to be
3169	exercised.
3170	(c) As used in this subsection, the term "plan of
3171	operation" means the plan developed pursuant to subsection (2).
3172	(d) Upon final action by the Governor with respect to a
3173	request to exercise the exemption authorized in this subsection,
3174	the department shall report such action, along with the original
3175	request and any modifications thereto, to the President of the
3176	Senate and the Speaker of the House of Representatives within 30
3177	days.
3178	Section 32. Effective July 1, 2026, paragraph (b) of
3179	subsection (4) of section 443.1113, Florida Statutes, is amended
3180	to read:
3181	443.1113 Reemployment Assistance Claims and Benefits
3182	Information System
3183	(4)
3184	(b) The department shall seek input on recommended
3185	enhancements from, at a minimum, the following entities:
3186	1. The Agency for State Systems and Enterprise Technology
3187	Florida Digital Service within the Department of Management
3188	Services.
3189	2. The General Tax Administration Program Office within the
3190	Department of Revenue.

Page 110 of 111

CODING: Words stricken are deletions; words underlined are additions.

SB 7026

	576-02644-25 20257026
3191	
3192	Department of Financial Services.
3193	Section 33. Effective July 1, 2026, subsection (5) of
3194	section 943.0415, Florida Statutes, is amended to read:
3195	943.0415 Cybercrime OfficeThere is created within the
3196	Department of Law Enforcement the Cybercrime Office. The office
3197	may:
3198	(5) Consult with the state chief information security
3199	officer of the Agency for State Systems and Enterprise
3200	Technology Florida Digital Service within the Department of
3201	Management Services in the adoption of rules relating to the
3202	information technology security provisions in s. 282.318.
3203	Section 34. Effective July 1, 2026, subsection (3) of
3204	section 1004.444, Florida Statutes, is amended to read:
3205	1004.444 Florida Center for Cybersecurity
3206	(3) Upon receiving a request for assistance from <u>a</u> the
3207	Department of Management Services, the Florida Digital Service,
3208	or another state agency, the center is authorized, but may not
3209	be compelled by the agency, to conduct, consult on, or otherwise
3210	assist any state-funded initiatives related to:
3211	(a) Cybersecurity training, professional development, and
3212	education for state and local government employees, including
3213	school districts and the judicial branch; and
3214	(b) Increasing the cybersecurity effectiveness of the
3215	state's and local governments' technology platforms and
3216	infrastructure, including school districts and the judicial
3217	branch.
3218	Section 35. Except as otherwise provided in this act, this
3219	act shall take effect July 1, 2025.

Page 111 of 111

CODING: Words stricken are deletions; words underlined are additions.

SB 7026