FOR CONSIDERATION By the Committee on Appropriations

576-02447-25 20257026pb

A bill to be entitled

An act relating to information technology; creating s. 20.70, F.S.; creating the Agency for State Systems and Enterprise Technology (ASSET); providing that the Governor and Cabinet are the head of the agency; establishing divisions and offices of the agency; providing for an executive director of the agency; providing that the executive director also serves as the state chief information officer; providing for the appointment and removal of such executive director; prohibiting the state chief information officer from having financial, personal, or business conflicts of interest related to certain vendors, contractors, and service providers of the state; requiring that the state chief information officer selection committee within ASSET be appointed and provide a specified number of nominees upon a vacancy of such officer; providing the composition of such committee; providing the qualifications for the state chief information officer; providing that persons who currently serve, or have served, as state agency heads are ineligible to serve as the state chief information officer; transferring the state chief information officer of the Department of Management Services to ASSET until the Governor and the Cabinet appoint a permanent officer; requiring that such appointment occur by a specified date; amending s. 97.0525, F.S.; requiring that the Division of Elections comprehensive risk assessment comply with the risk assessment methodology

developed by ASSET; amending s. 112.22, F.S.; defining the term "ASSET"; deleting the term "department"; revising the definition of the term "prohibited application"; authorizing public employers to request a certain waiver from ASSET; requiring ASSET to take specified actions; deleting obsolete language; requiring ASSET to adopt rules; amending s. 119.0725, F.S.; providing that confidential and exempt information must be made available to ASSET; amending s. 216.023, F.S.; requiring agencies and the judicial branch to include a cumulative inventory and a certain status report of specified projects with their legislative budget requests; defining the term "technology-related project"; deleting a provision requiring state agencies and the judicial branch to include a cumulative inventory and a certain status report of specified projects as part of a budget request; conforming a cross-reference; amending s. 282.0041, F.S.; deleting and revising definitions; defining the terms "ASSET" and "technical debt"; amending s. 282.0051, F.S.; deleting obsolete language; revising the powers, duties, and functions of the Department of Management Services, through the Florida Digital Service; deleting a requirement that the state chief information officer, in consultation with the Secretary of Management Services, designate a state chief data officer; deleting requirements of the department, acting through the Florida Digital Service, relating to the use of appropriated funds for

certain actions; deleting provisions related to information technology projects that have a total project cost in excess of $10 million; providing for the future repeal of the section; deleting a requirement to adopt rules; repealing s. 282.00515, F.S., relating to duties of Cabinet agencies; creating s. 282.006, F.S.; requiring ASSET to operate as the state enterprise organization for information technology governance and as the lead entity responsible for understanding needs and environments, creating standards and strategy, supporting state agency technology efforts, and reporting on the state of information technology in this state; providing legislative intent; requiring ASSET to establish the strategic direction of information technology in the state; requiring ASSET to develop and publish information technology policy for a specified purpose; requiring that such policy be updated as necessary to meet certain requirements and advancements in technology; requiring ASSET to take specified actions related to oversight of the state's technology enterprise; requiring ASSET to produce specified reports, recommendations, and analyses and provide such reports, recommendations, and analyses to the Governor, the Commissioner of Agriculture, the Chief Executive Officer, the Attorney General, and the Legislature by specified dates and at specified intervals; providing requirements for such reports; requiring ASSET to conduct a market analysis at a

certain interval beginning on a specified date; providing requirements for the market analysis; requiring that each market analysis be used to prepare a strategic plan for specified purposes; requiring that copies of the market analysis and strategic plan be submitted by a specified date; authorizing ASSET to adopt rules; creating s. 282.0061, F.S.; providing legislative intent; requiring ASSET to complete a certain full baseline needs assessment of state agencies, develop a specified plan to conduct such assessments, and submit such plan to the Governor, the Commissioner of Agriculture, the Chief Financial Officer, the Attorney General, and the Legislature within a specified timeframe; requiring ASSET to support state agency strategic planning efforts and assist such agencies with a certain phased roadmap; providing requirements for such roadmaps; requiring ASSET to make recommendations for standardizing data across state agencies for a specified purpose and identify any opportunities for standardization and consolidation of information technology services across state agencies and support specified functions; requiring ASSET to develop standards for use by state agencies and enforce consistent standards and promote best practices across all state agencies; requiring ASSET to provide a certain report to the Governor, the Commissioner of Agriculture, the Chief Financial Officer, the Attorney General, and the Legislature by a specified date; providing requirements of the

report; providing the duties and responsibilities of ASSET related to state agency technology projects; requiring ASSET, in consultation with state agencies, to create a methodology, approach, and applicable templates and formats for identifying and collecting information technology expenditure data at the state agency level; requiring ASSET to obtain, review, and maintain records of the appropriations, expenditures, and revenues for information technology for each state agency; requiring ASSET to prescribe the format for state agencies to provide financial information to ASSET for inclusion in a certain annual report; requiring state agencies to submit such information by a specified date annually; requiring that such information be reported to ASSET to determine all costs and expenditures of information technology assets and resources provided to state agencies; requiring ASSET to work with state agencies to provide alternative standards, policies, or requirements under specified circumstances; creating s. 282.0062, F.S.; establishing workgroups within ASSET to facilitate coordination with state agencies; providing for the membership and duties of such workgroups; creating s. 282.0063, F.S.; requiring ASSET to perform specified actions to develop and manage career paths, progressions, and training programs for the benefit of state agency personnel; creating s. 282.0064, F.S.; requiring ASSET, in coordination with the Department of Management Services, to establish a policy for all

information technology-related solicitations, contracts, and procurements; providing requirements for the policy related to state term contracts, all contracts, and information technology projects that require oversight; prohibiting entities providing independent verification and validation from having certain interests, responsibilities, or other participation in the project; providing the primary objective of independent verification and validation; requiring the entity performing such verification and validation to provide specified regular reports and assessments; requiring the Division of State Purchasing within the Department of Management Services to coordinate with ASSET on state term contract solicitations and invitations to negotiate; requiring ASSET to evaluate vendor responses and answer vendor questions on such solicitations and invitations; creating s. 282.0065, F.S.; requiring ASSET to establish, maintain, and manage a certain test laboratory, beginning at a specified time; providing the purpose of the laboratory; requiring ASSET to take specified actions relating to the laboratory; creating s. 282.0066, F.S.; requiring ASSET to develop, implement, and maintain a certain library; providing requirements for the library; requiring ASSET to establish procedures that ensure the integrity, security, and availability of the library; requiring ASSET to regularly update documents and materials in the library to reflect current state

and federal requirements, industry best practices, and emerging technologies; requiring state agencies to reference and adhere to the policies, standards, and guidelines of the library in specified tasks; requiring ASSET to create mechanisms for state agencies to submit feedback, request clarifications, and recommend updates; authorizing state agencies to request exemptions to specific policies, standards, or guidelines under specified circumstances; providing the mechanism for a state agency to request such exemption; requiring ASSET to review the request and make a recommendation to the state chief information officer; requiring the state chief information officer to present the exemption to the chief information officer workgroup; requiring that approval of the exemption be by majority vote; requiring that state agencies granted an exemption be reviewed periodically to determine whether such exemption is necessary or if compliance can be achieved; amending s. 282.318, F.S.; revising the duties of the Department of Management Services, acting through the Florida Digital Service, relating to cybersecurity; requiring state agencies to report all ransomware incidents to the state chief information security officer instead of the Cybersecurity Operations Center; requiring the state chief information security officer, instead of the Cybersecurity Operations Center, to notify the Legislature of certain incidents; requiring state agencies to notify the state chief information

security officer within specified timeframes after the discovery of a specified cybersecurity incident or ransomware incident; requiring the state chief information security officer, instead of the Cybersecurity Operations Center, to provide a certain report on a quarterly basis to the Legislature; revising the actions that state agency heads are required to perform relating to cybersecurity; reducing the timeframe that the state agency strategic cybersecurity plan must cover; requiring that a specified comprehensive risk assessment be done biennially; providing requirements for such assessment; revising the definition of the term "state agency"; providing that ASSET is the lead entity responsible for establishing enterprise technology and cybersecurity standards and processes and security measures that comply with specified standards; requiring ASSET to adopt specified rules; requiring that ASSET take specified actions; revising the responsibilities of the state chief information security officer; requiring that ASSET develop and publish a specified framework that includes certain guidelines and processes for use by state agencies; requiring that ASSET, in consultation with the state chief information technology procurement officer, establish specified procedures for procuring information technology commodities and services; requiring ASSET, thorough the state chief information security officer and the Division of Enterprise

Information Technology Workforce Development, to provide a certain annual training to specified persons; conforming provisions to changes made by the act; amending s. 282.3185, F.S.; requiring the state chief information security officer to perform specified actions relating to cybersecurity training for state employees; requiring local governments to notify the state chief information security officer of compliance with specified provisions as soon as possible; requiring local governments to notify the state chief information security officer, instead of the Cybersecurity Operations Center, of cybersecurity or ransomware incidents; revising the timeframes in which such notifications must be made; requiring the state chief information security officer to notify the state chief information officer, the Governor, the Commissioner of Agriculture, the Chief Financial Officer, the Attorney General, and the Legislature of certain incidents within a specified timeframe; authorizing local governments to report certain cybersecurity incidents to the state chief information security officer instead of the Cybersecurity Operations Center; requiring the state chief information security officer to provide a certain consolidated incident report within a specified timeframe to the Governor, the Commissioner of Agriculture, the Chief Financial Officer, the Attorney General, and the Legislature; conforming provisions to changes made by the act; requiring the state chief

information security officer to establish certain guidelines and processes by a specified date; conforming cross-references; repealing s. 282.319, F.S., relating to the Florida Cybersecurity Advisory Council; establishing positions within ASSET; establishing the Division of Enterprise Information Technology Services and the Division of Enterprise Information Technology Purchasing and associated bureaus; providing the responsibilities of the bureaus; establishing the chief information officer policy workgroup; providing the membership, purpose, chair, and duties of the workgroup; providing for the expiration of the workgroup upon completion of its duties; amending s. 282.201, F.S.; revising requirements of the state data center; abrogating the scheduled repeal of the Division of Emergency Management's exemption from using the state data center; deleting Department of Management Services responsibilities related to the state data center; deleting provisions relating to contracting with the Northwest Regional Data Center; transferring, renumbering, and amending s. 1004.649, F.S.; requiring the Northwest Regional Data Center, by a specified date annually, to provide the projected costs of providing data center services for the following fiscal year to the Office of Policy and Budget in the Executive Office of the Governor and to the chairs of the legislative appropriations committees; deleting a requirement that the data center prepare and submit

certain invoices to the Department of Management Services for approval; conforming a cross-reference; amending s. 20.22, F.S.; deleting the Florida Digital Service from the list of divisions, programs, and services of the Department of Management Services; amending s. 282.802, F.S.; providing that the Government Technology Modernization Council is located within ASSET; providing that the state chief information officer, or his or her designee, is the ex officio executive director of the council; conforming provisions to changes made by the act; requiring the council annually to submit to the Commissioner of Agriculture, the Chief Financial Officer, and the Attorney General certain legislative recommendations; amending s. 282.604, F.S.; requiring ASSET, with input from stakeholders, to adopt rules; amending s. 287.0591, F.S.; requiring the state chief information officer, instead of the Florida Digital Service, to participate in certain solicitations; amending s. 288.012, F.S.; conforming a cross-reference; amending 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:

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.

(b) The Office of Information Technology.

(c) Beginning July 1, 2026:

1. The Division of Enterprise Data and Interoperability.

2. The Division of Enterprise Security.

3. The Division of Enterprise Information Technology Services.

4. The Division of Enterprise Information Technology Purchasing.

5. The Division of Enterprise Information Technology Workforce Development.

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

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

(3) STATE CHIEF INFORMATION OFFICER SELECTION COMMITTEE.—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Public sector information technology management by 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:

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 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 appointed pursuant to s. 20.70, Florida Statutes, the current state chief information officer of the Department of Management Services shall be transferred to the Agency for State Systems and Enterprise Technology and serve as interim state chief information officer. A state chief information officer for the Agency for State Systems and Enterprise Technology must be appointed by the Governor and Cabinet by January 2, 2026. Appointments to the state chief information officer selection committee must be made by August 1, 2025.

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

97.0525 Online voter registration.—

(3)

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

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

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

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

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

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

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

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

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

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

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

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

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

c. Conducting cyber-espionage against a public employer;

d. Conducting surveillance and tracking of individual users; or

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

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

(2)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

administer this section.

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

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

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

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

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

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

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

(a) The name of the technology system.

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

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

(d) The initiation date of the project.

(e) The key performance indicators for the project.

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

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

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

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

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

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

Statutes, are amended to read:

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

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

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

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

3. Details on trust funds and fees.

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

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

6. Information resource requests.

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

8. An evaluation of major outsourcing and privatization

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

282.0051 Department of Management Services; Florida Digital

Service; powers, duties, and functions.—

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

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

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

(c) Direct the state chief information security officer to provide a consolidated cybersecurity incident report by the 30th day after the end of each quarter to the interim state chief information officer, 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 ~~Develop and publish information technology policy for the management of the state's information technology resources~~.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

enterprise, ASSET shall:

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

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

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

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

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

a. Data models and taxonomies.

b. Master data management.

c. Data integration and interoperability.

d. Data security and encryption.

e. Bot prevention and data protection.

f. Data backup and recovery.

g. Application portfolio and catalog requirements.

h. Application architectural patterns and principles.

i. Technology and platform standards.

j. Secure coding practices.

k. Performance and scalability.

l. Cloud infrastructure and architecture.

m. Networking, connectivity, and security protocols.

n. Authentication, authorization, and access controls.

o. Disaster recovery.

p. Quality assurance.

q. Testing methodologies and measurements.

r. Logging and log retention.

s. Application and use of artificial intelligence.

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

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

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

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

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

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

(5) ASSET shall produce the following reports and provide them to 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:

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

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

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

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

a. Total number of full-time equivalent positions.

b. Total amount of salary.

c. Total amount of benefits.

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

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

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

g. Total amount of expenditures for hardware.

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

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

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

k. Total amount of expenditures for administrative costs.

4. Consolidated information for the previous fiscal year

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

282.0061 ASSET support of state agencies; information technology procurement and projects.—

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

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

(2) NEEDS ASSESSMENTS.—

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

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

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

(c) ASSET shall develop a plan and schedule to conduct the initial full baseline needs assessments. By October 1, 2026, ASSET shall submit the plan to 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.

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

(3) STANDARDIZATION.—ASSET shall:

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

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

1. Improved interoperability, security, scalability,

maintainability, and cost efficiency; and

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

(4) DATA MANAGEMENT.—

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

(b) ASSET shall establish a methodology and strategy for implementing statewide master data management and submit a report to 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 by December 1, 2028. The report must include the vision, goals, and benefits of implementing a statewide master data management initiative, an analysis of the current state of data management, and the recommended strategy, methodology, and estimated timeline and resources needed at a state agency and enterprise level to accomplish the initiative.

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

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

(b) Establish best practices and enterprise procurement

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

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

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

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

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

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

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

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

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

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

(g) Perform project oversight on all state agency information technology projects that have total project costs of $10 million or more. ASSET shall report by the 30th day after the end of each quarter 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 on any information technology project that ASSET identifies as high-risk. The report must include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project, and a recommendation for corrective actions required, including suspension or termination of the project.

(6) INFORMATION TECHNOLOGY FINANCIAL DATA.—

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

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

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

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

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

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

(1) CHIEF INFORMATION OFFICER WORKGROUP.—

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

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

(2) ENTERPRISE DATA AND INTEROPERABILITY WORKGROUP.—

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

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

(3) ENTERPRISE SECURITY WORKGROUP.—

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

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

(4) ENTERPRISE INFORMATION TECHNOLOGY OPERATIONS

WORKGROUP.—

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

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

(5) ENTERPRISE INFORMATION TECHNOLOGY QUALITY ASSURANCE WORKGROUP.—

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

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

(6) ENTERPRISE INFORMATION TECHNOLOGY PROJECT MANAGEMENT WORKGROUP.—

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

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

(7) ENTERPRISE INFORMATION TECHNOLOGY CONTRACT MANAGEMENT WORKGROUP.—

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

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

(8) ENTERPRISE INFORMATION TECHNOLOGY PURCHASING WORKGROUP.—

(a) The enterprise information technology purchasing

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

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

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

282.0063 State information technology professionals career paths and training.—

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

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

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

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

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

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

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

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

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

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

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

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

282.0064 Information technology contract policy.—

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

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

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

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

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

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

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

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

(b) Requirements to be included in solicitations.

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

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

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

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

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

(b) The primary objective of independent verification and

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

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

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

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

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

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

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

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

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

282.0065 ASSET information technology test laboratory.—

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

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

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

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

(3) ASSET shall:

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

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

(c) Support the development of requirements for state

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

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

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

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

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

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

282.0066 Enterprise Information Technology Library.—

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

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

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

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

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

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

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

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

b. The reason compliance is not feasible or practical.

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

d. The anticipated duration of the exemption.

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

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

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

282.318 Cybersecurity.—

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

Digital Service, shall also:

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

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

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

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

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

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

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

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

~~events, continuous security monitoring, and defined detection 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.~~

~~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.

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

public health or safety; national, state, or local security; 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 confidence.

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

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

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

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

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

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

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

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

(II) The state chief information security officer ~~Cybersecurity Operations Center~~ shall 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.

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

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

2.~~10.~~ Incorporating information obtained through detection

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

3.~~11.~~ Developing agency strategic and operational cybersecurity plans required pursuant to this section.

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

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

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

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

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

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

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

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

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

(c) Submit to the state chief information security officer ~~department~~ 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 ~~department, through the Florida Digital Service~~.

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

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

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

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

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

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

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

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

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

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

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

282.318 Cybersecurity.—

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

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

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

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

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

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

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

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

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

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

technology resources.

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

6. Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection 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.

9. Establishing a cybersecurity incident reporting process that includes procedures for notifying ASSET ~~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 public health or safety; national, state, or local security; 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 confidence.

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

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

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

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

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

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

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

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

(II) The state chief information security officer shall 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.

d. A state agency shall report a cybersecurity incident determined by the state agency to be of severity level 1 or 2 to the state chief information security officer and the Cybercrime Office of the Department of Law Enforcement as soon as possible, but no later than 96 hours after the discovery of the cybersecurity incident and no later than 72 hours after the discovery of the ransomware incident. The report must contain 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.

10.~~2.~~ Incorporating information obtained through detection and response activities into the agency's cybersecurity incident response plans.

11.~~3.~~ Developing agency strategic and operational cybersecurity plans required pursuant to this section.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

282.3185 Local government cybersecurity.—

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

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

(3) CYBERSECURITY TRAINING.—

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

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

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

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

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

(4) CYBERSECURITY STANDARDS.—

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

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

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

(d) Each local government shall notify the state chief

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

(5) INCIDENT NOTIFICATION.—

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

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

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

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

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

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

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

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

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

2. The state chief information security officer ~~Cybersecurity Operations Center~~ shall notify the state chief information officer, 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 of any severity level 3, 4, or 5 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 2 as provided in s. 282.318(3)(b) ~~s. 282.318(3)(c)~~ to the state chief information security officer ~~Cybersecurity Operations Center~~, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government. The report shall contain the information required in paragraph (a).

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

~~a quarterly basis~~ to 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~~, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory Council may not contain the name of any local government, network information, or system identifying information but must contain sufficient relevant information to allow the Florida Cybersecurity Advisory Council to fulfill its responsibilities as required in s. 282.319(9)~~.

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

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

282.3185 Local government cybersecurity.—

(3) CYBERSECURITY TRAINING.—

(a) The state chief information security officer shall:

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

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

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

(5) INCIDENT NOTIFICATION.—

(b)1. A local government shall report all ransomware incidents and any cybersecurity incident determined by the local 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 security officer, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government as soon as possible but no later than 12 hours after discovery of the cybersecurity incident and no later than 6 hours after discovery of the ransomware incident. The report must contain the information required in paragraph (a).

2. The state chief information security officer shall notify the state chief information officer, the Governor, the Commission of Agriculture, the Chief Financial Officer, the Attorney General, 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 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 2 as provided in s. 282.318(3)(c) ~~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 jurisdiction over the local government. The report shall contain the information required in paragraph (a).

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

Section 23. (1) POSITIONS.—

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

1. Chief operations officer.

2. Chief information officer.

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

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

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

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

development.

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

3. State chief data officer and the following:

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

(I) Personally identifiable information.

(II) Protected health information.

(III) Criminal justice information services.

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

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

5. State chief technology officer and the following:

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

follows:

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

(A) Two dedicated to the Department of Health.

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

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

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

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

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

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

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

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

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

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

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

(B) Two dedicated to the Department of Corrections.

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

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

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

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

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

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

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

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

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

(A) Two dedicated to the Department of Transportation.

(B) Two dedicated to the Department of State.

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

(D) Two dedicated to the Department of Commerce.

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

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

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

and transportation and economic development.

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

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

(2) BUREAUS.—

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

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

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

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

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

(b) The Division of Enterprise Information Technology Purchasing shall include:

1. The Bureau of Enterprise Information Technology Procurement Services, responsible for procurement activities established under s. 282.006, Florida Statutes.

2. The Bureau of Enterprise Information Technology Procurement Policy and Oversight, responsible for activities established under s. 282.006, Florida Statutes.

(3) WORKGROUP.—

(a) The chief information officer policy workgroup shall be composed of all state agency chief information officers.

(b) The purpose of the workgroup is to provide the Legislature with input and feedback regarding the structure, budget, and governance of the Agency for State Systems and Enterprise Technology.

(c) The chair of the workgroup shall be the interim state chief information officer.

(d) The voting members of the workgroup shall include the chair of the workgroup and the chief information officers from the Department of Financial Services, the Department of Agriculture and Consumer Services, and the Department of Legal Affairs.

(e) The chair of the workgroup shall submit a report to 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 which includes recommendations and justifications for changes by December 1, 2025. The final report must be voted on and accepted by a unanimous vote of the voting members of the workgroup.

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

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

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

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

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

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

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

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

~~a term exceeding 3 years and at a minimum must:~~

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

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

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

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

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

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

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

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

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

~~10. Provide for mediation of disputes by the Division of~~

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Identify the scope of work;

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

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

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

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

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

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

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

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

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

Northwest Regional Data Center on behalf of the customer entity.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Digital Service.

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

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

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

(a) Facilities Program.

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

~~(c)~~ Workforce Program.

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

2. Federal Property Assistance Program.

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

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

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

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

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

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

282.802 Government Technology Modernization Council.—

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

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

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

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

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

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

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

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

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

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

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

(8) ~~By December 31, 2024, and~~ Each December 31 ~~thereafter,~~ the council shall submit to 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 any legislative recommendations considered necessary by the council to modernize government technology, including:

(a) Recommendations for policies necessary to:

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

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

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

(b) Any other information the council considers relevant.

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

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

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

287.0591 Information technology; vendor disqualification.—

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

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

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

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

(a) The department may exercise such exemptions only upon 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 continuing authority for the department to exercise the exemption, but only in the context and upon the terms originally granted. Any modification of the approved plan of operation with respect to an exemption contained therein must be resubmitted to the Governor for his or her approval. An approval granted to exercise an exemption in any other context shall be restricted to the specific instance for which the exemption is to be exercised.

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

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

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

443.1113 Reemployment Assistance Claims and Benefits Information System.—

(4)

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

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

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

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

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

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

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

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

1004.444 Florida Center for Cybersecurity.—

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

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

(b) Increasing the cybersecurity effectiveness of the

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

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