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

576-02812-26 2026480c2

A bill to be entitled

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

permanent officer; requiring that such appointment occur by a specified date; amending s. 20.055, F.S.; requiring agency inspectors general to review and report whether certain agency practices are consistent with specified reporting requirements and standards; requiring such inspectors general to prepare and submit a certain compliance report to certain persons by a specified date annually; requiring the chief inspector general to review certain reports and prepare a consolidated report; requiring that such report be submitted to the Executive Office of the Governor and the Legislature annually by a specified date; requiring certain agency heads to submit certain reports to the Executive Office of the Governor and the Legislature annually 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 DIGIT; amending s. 112.22, F.S.; defining the term "DIGIT"; deleting the term "department"; revising the definition of the term "prohibited application"; authorizing public employers to request a certain waiver from DIGIT; requiring DIGIT to take specified actions; deleting obsolete language; requiring DIGIT to adopt rules; amending s. 119.0725, F.S.; requiring that certain confidential and exempt information be made available to DIGIT; amending s. 216.023, F.S.; 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; deleting provisions relating to ongoing technology-related projects; conforming a cross-reference; amending s. 282.0041, F.S.; deleting and revising definitions; defining the terms "DIGIT" and "technical debt"; amending s. 282.00515, F.S.; authorizing the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services to adopt alternative standards that must be based on specified industry-recognized best practices and standards; requiring the departments to evaluate the adoption of such standards on a case-by-case basis; requiring the departments to follow specified standards under certain circumstances; requiring the departments to conduct a certain full baseline needs assessment; authorizing the departments to contract with DIGIT to assist or complete such assessment; requiring the departments to each produce certain phased roadmaps that must be submitted annually with specified budget requests; authorizing the departments to contract with DIGIT to assist or complete such roadmaps; authorizing the departments to contract with DIGIT for specified services; requiring the departments to use certain information technology reports and follow a specified reporting process; requiring the departments to submit a certain report annually by a specified date to the Governor and the Legislature; revising applicability; authorizing DIGIT to perform project oversight on

information technology projects of the departments which have a specified project cost; requiring that such projects comply with certain standards; requiring DIGIT to report periodically to the Legislature high-risk information technology projects; specifying report requirements; requiring state agencies to consult with DIGIT and work cooperatively with certain departments under specified circumstances; revising cross-references; creating s. 282.006, F.S.; requiring DIGIT 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 DIGIT to establish the strategic direction of information technology in the state; requiring DIGIT to develop and publish an information technology policy for a specified purpose; requiring that such policy be updated as necessary to meet certain requirements and reflect advancements in technology; requiring DIGIT, in coordination with certain subject matter experts, to develop, publish, and maintain specified enterprise architecture; requiring DIGIT to take specified actions related to oversight of the state’s technology enterprise; requiring DIGIT to develop open data standards and technologies for use by state agencies; requiring DIGIT to develop certain

testing, best practices, and standards; specifying such best practices and standards; requiring DIGIT to produce specified reports and provide such reports to the Governor and the Legislature by specified dates and at specified intervals; specifying requirements for such reports; requiring DIGIT to conduct a market analysis at a certain interval beginning on a specified date; specifying requirements for the market analysis; requiring that each market analysis be used to prepare a strategic plan for specified purposes; requiring that the market analysis and strategic plan be submitted by a specified date; requiring DIGIT to develop, implement, and maintain a certain library; specifying requirements for the library; requiring DIGIT to establish procedures that ensure the integrity, security, and availability of the library; requiring DIGIT to regularly update documents and materials in the library to reflect current state and federal requirements, industry best practices, and emerging technologies; requiring DIGIT to create mechanisms for state agencies to submit feedback, request clarification, and recommend updates; requiring state agencies to actively participate and collaborate with DIGIT to achieve certain objectives and to reference and adhere to the policies, standards, and guidelines of the library in specified tasks; 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 exemptions; requiring DIGIT 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 whether compliance can be achieved; authorizing DIGIT to adopt rules; creating s. 282.0061, F.S.; providing legislative intent; requiring DIGIT 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 and the Legislature within a specified timeframe; requiring DIGIT to support state agency strategic planning efforts and assist agencies with production of a certain phased roadmap; specifying requirements for such roadmaps; requiring DIGIT to make recommendations for standardizing data across state agencies for a specified purpose, identify any opportunities for standardization and consolidation of information technology services across state agencies, support specified functions, review all state agency legislative budget requests for compliance, and provide a certain review to the Office of Policy and Budget in the Executive Office of the Governor; requiring DIGIT to develop standards for use by state

agencies which support specified best practices for data management at the state agency level; requiring DIGIT to provide a certain report to the Governor and the Legislature by a specified date; specifying requirements for the report; providing the duties and responsibilities of DIGIT related to state agency technology projects; requiring DIGIT, 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 DIGIT to continuously obtain, review, and maintain records of the appropriations, expenditures, and revenues for information technology for each state agency; requiring DIGIT to prescribe the format for state agencies to provide financial information to DIGIT for inclusion in a certain annual report; requiring state agencies to submit such information by a specified date annually; requiring DIGIT to work with state agencies to provide alternative standards, policies, or requirements under specified circumstances; creating s. 282.0062, F.S.; establishing workgroups within DIGIT to facilitate coordination with state agencies; providing for the membership and duties of such workgroups; requiring the appropriate staff of the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services to participate in specified workgroups; authorizing such

staff to participate in specified workgroups and any other workgroups as authorized by their respective elected official; creating s. 282.0063, F.S.; requiring DIGIT to perform specified actions to develop and manage career paths, progressions, and training programs for the benefit of state agency personnel; requiring DIGIT to consult with specified entities to implement specified provisions; creating s. 282.0064, F.S.; requiring DIGIT, in coordination with the Department of Management Services, to establish a policy for all information technology-related solicitations, contracts, and procurements; specifying 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 DIGIT on state term contract solicitations and invitations to negotiate; specifying the scope of the coordination; requiring DIGIT to evaluate vendor responses and assist with answers to vendor questions on such solicitations and invitations; authorizing the

Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services to adopt alternative information technology policy; providing requirements for adopting such alternative policy; amending s. 282.318, F.S.; providing that DIGIT is the lead entity responsible for establishing enterprise technology and cybersecurity standards and processes and security measures that comply with specified standards; requiring DIGIT to adopt specified rules; requiring DIGIT to take specified actions; revising the responsibilities of the state chief information security officer; revising the guidelines and processes for state agency cybersecurity governance frameworks; requiring state agencies to report all ransomware incidents to the state chief information security officer instead of the Cybersecurity Operations Center; requiring state agencies to also notify the Northwest Regional Data Center of such incidents under specified conditions; 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 state agencies to also notify the Northwest Regional Data Center of such incidents under specified conditions; 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; revising the timeframe that the state agency strategic cybersecurity plan must cover; requiring that a specified comprehensive risk assessment be completed biennially; authorizing such assessment to be completed by an independent third party; requiring the third party to attest to the validity of the findings; specifying requirements for the comprehensive risk assessment; providing that confidential and exempt records be made available to the state chief information security officer and Legislature; 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; deleting obsolete language; 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

Governor 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 Legislature; requiring the state chief information security officer to establish certain guidelines and processes by a specified date; conforming provisions to changes made by the act; repealing s. 282.319, F.S., relating to the Florida Cybersecurity Advisory Council; amending s. 282.201, F.S.; establishing the state data center within the Northwest Regional Data Center; requiring the Northwest Regional Data Center to meet or exceed specified information technology standards; 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 the Department of Management Services' responsibilities related to the state data center; deleting provisions relating to contracting with the Northwest Regional Data Center; creating s. 282.2011, F.S.; designating the Northwest Regional Data Center as the state data center for all state agencies; requiring the data center to engage in specified actions; requiring the Department of Law Enforcement to serve as the arbiter of certain

disputes in accordance with the federal criminal justice information guidelines; prohibiting state agencies from terminating services with the data center without giving written notice within a specified timeframe, procuring third-party cloud-computing services without evaluating the data center's cloud-computing services, and exceeding a specified timeframe to remit payments for services provided by the data center; specifying circumstances under which the data center's authorization to provide services may be terminated; providing that the data center has a specified timeframe to provide for the transition of state agency customers to a qualified alternative cloud-based data center that meets specified standards; providing that the data center is the lead entity responsible for creating, operating, and managing the Florida Behavioral Health Care Data Repository; providing the purpose of the repository; requiring the data center, in collaboration with the Data Analysis Committee of the Commission on Mental Health and Substance Use Disorder, to develop a specified plan; requiring, beginning on a specified date, the data center to submit a certain report annually to the Governor and the Legislature; providing for a transition to an alternative cloud-based data center under specified circumstances; revising the information the plan identifies and documents; amending s. 282.206, F.S.; requiring state agencies to submit a certain strategic plan to DIGIT

and the Northwest Regional Data Center annually by a specified date; amending s. 1004.649, F.S.; creating the Northwest Regional Data Center at Florida State University; conforming provisions to changes made by the act; creating s. 287.0583, F.S.; requiring that contracts for information technology commodities and services ensure extraction of data, certain documentation, assistance and support, and anticipated fees; amending s. 287.0591, F.S.; requiring the Department of Management Services to coordinate with DIGIT in specified solicitations; specifying the scope of the coordination; requiring agencies to maintain copies of certain documents when issuing a request for quote for state term contracts within specified threshold amounts; providing that agencies that issue requests for quotes in excess of certain thresholds are subject to specified public records requirements; requiring such agencies to publish specified information; requiring such agencies to maintain copies of certain documentation for a specified timeframe; providing that use of a request for quote is not subject to certain protest provisions; authorizing agencies to request certain services from DIGIT; requiring the department to prequalify firms and individuals who provide information technology commodities; authorizing such firms and individuals to submit responses to requests for quotes; amending s. 20.22, F.S.; conforming provisions to changes made by the act; amending s. 282.802, F.S.; providing that the

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

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

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

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

read:

14.205 Division of Integrated Government Innovation and Technology.—

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

(2)(a) The director of the division shall serve as the state chief information officer. The director shall be appointed by the Governor, subject to confirmation by the Senate. 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.

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

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

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

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

2. 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:

a. 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;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

20.055 Agency inspectors general.—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Section 5. 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 Division of Integrated Government Innovation and Technology within the Executive Office of the Governor ~~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 6. 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) "DIGIT" means the Division of Integrated Government Innovation and Technology within the Executive Office of the Governor ~~"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 that DIGIT ~~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 DIGIT ~~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 DIGIT ~~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) DIGIT ~~The department~~ shall do all of the following:

(a) Compile and maintain a list of prohibited applications and publish the list on its website. DIGIT ~~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 DIGIT ~~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)~~ DIGIT ~~The department~~ shall adopt rules necessary to administer this section.

Section 7. 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 Division of Integrated Government Innovation and Technology within the Executive Office of the Governor ~~Florida Digital Service within the Department of Management Services~~, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.

Section 8. 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 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 an inventory of all ongoing technology-related projects that have a cumulative estimated or realized cost of more than $1 million. 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, 2026.~~

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

section are amended, to read:

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

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

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

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

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

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

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

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

282.00515 Duties of Cabinet agencies.—

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

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

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

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

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

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

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

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

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

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

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

(8) Notwithstanding s. 282.0061(5)(h), DIGIT may perform project oversight only on information technology projects of the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services which have a 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 DIGIT. DIGIT shall report by the 30th day after the end of each quarter to the President of the Senate and the Speaker of the House of Representatives on any information technology project under this subsection which DIGIT 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 any corrective action required, including suspension or termination of the project.

(9) 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 Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services, the state agency must consult with DIGIT regarding the risks and other effects of such project on the information technology systems of

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

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

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

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

(2) The Legislature intends for DIGIT 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) DIGIT shall establish the strategic direction of information technology for state agencies. DIGIT 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) DIGIT shall, in coordination with state agency technology subject matter experts, develop, publish, and maintain an enterprise architecture that:

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

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

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

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

1. Data models and taxonomies.

2. Master data management.

3. Data integration and interoperability.

4. Data security and encryption.

5. Bot prevention and data protection.

6. Data backup and recovery.

7. Application portfolio and catalog requirements.

8. Application architectural patterns and principles.

9. Technology and platform standards.

10. Secure coding practices.

11. Performance and scalability.

12. Cloud infrastructure and architecture.

13. Networking, connectivity, and security protocols.

14. Authentication, authorization, and access controls.

15. Disaster recovery.

16. Quality assurance.

17. Testing methodologies and measurements.

18. Logging and log retention.

19. Application and use of artificial intelligence.

(5) DIGIT shall develop open data technical standards and terminologies for use by state agencies. DIGIT shall 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:

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

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

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

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

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

(a) Annually by December 15, an enterprise analysis report for state agencies which 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. As used in this paragraph, 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.

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

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

2. Information technology services needed to be designed, delivered, and managed as state agency 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, DIGIT shall conduct a market analysis to determine whether the:

a. Information technology resources across state agencies 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. State agencies are 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, including, but not limited to, proposed acquisitions of new services or technologies and approaches to the implementation of any new services or technologies.

(7)(a) DIGIT 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 online library must be accessible and searchable by all state agencies and the Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer

Services through a secure authentication system. 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.

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

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

(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 any agency-specific statutory requirement. The state agency requesting an exemption must submit a formal justification to DIGIT 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 control or alternative measure the state agency will implement to mitigate associated risks.

d. The anticipated duration of the exemption.

2. DIGIT 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 and include conditions and expiration dates.

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

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

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

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

(1) LEGISLATIVE INTENT.—The Legislature intends for DIGIT 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. DIGIT assistance and support must allow for adaptability to emerging technologies and organizational needs while maintaining compliance with industry best practices. DIGIT may not prescribe specific tools, platforms, or vendors.

(2) NEEDS ASSESSMENTS.—

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

(b) In assessing the existing technical debt portion of the needs assessment, DIGIT 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) DIGIT shall develop a plan and schedule to conduct the initial full baseline needs assessments. By October 1, 2027, DIGIT shall submit the plan to the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(d) DIGIT 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 latest version of the Capability Maturity Model Integration. 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.—DIGIT shall:

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

(b) Identify any opportunities in such enterprise analysis report for state agencies 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.

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

funding decisions in the Governor's recommended budget.

(4) DATA MANAGEMENT.—

(a) DIGIT 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) DIGIT shall establish a methodology and strategy for implementing statewide master data management and submit a report to the Governor, the President of the Senate, and the Speaker of the House of Representatives by December 1, 2029. 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.—DIGIT 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 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 project planning and implementation, including criteria for effective project management and oversight. State agencies shall 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 assess the progress and risks of an information technology project based on a defined and documented project scope, to include the number of impacted stakeholders, cost, and schedule, to determine whether the project is performing as planned and delivering the intended outcomes.

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

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

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

architecture standards.

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

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

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

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

3. Planning and scheduling.

4. Stakeholder engagement.

5. Risk assessment.

6. Procurement strategy.

7. Project governance definition.

8. System design and requirements.

9. Change management.

10. Monitoring and reporting.

11. Postimplementation review and planning.

12. Solicitation documentation.

(f) 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.

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

(h) Perform project oversight on all state agency information technology projects that have total project costs of $10 million or more. DIGIT shall report by the 30th day after the end of each quarter 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 DIGIT identifies as high-risk due to the project exceeding the acceptable project variance thresholds provided in the project management and oversight standards. The report must include a risk assessment, including fiscal risks associated with proceeding to the next stage of the project, a list of all projects with a performance deficiency, reported pursuant to s. 287.057(26)(d)1., which has not been corrected as of the end of the reporting period, and a recommendation for corrective actions required, including suspension or termination of the project.

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

of noncompliance with the standards developed and adopted by DIGIT.

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

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

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

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

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

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

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

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

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

(6) INFORMATION TECHNOLOGY FINANCIAL DATA.—

(a) In consultation with state agencies, DIGIT 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. DIGIT shall continuously obtain, review, and maintain records of the appropriations, expenditures, and revenues for information technology for each state agency.

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

(7) FEDERAL CONFLICTS.—DIGIT must 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 any state agency or loss of federal funding.

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

282.0062 DIGIT workgroups.—The following workgroups are established within DIGIT 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 information security officer representatives from all state agencies, shall consider and make recommendations to the state chief information 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 information 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 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 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 enterprise software testing and quality assurance standards.

(5) 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 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 project management and oversight.

(6) 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 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 technology evaluation, purchasing, and cost savings.

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

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

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

282.0063 State information technology professionals career paths and training.—

(1) DIGIT 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, DIGIT shall:

(a) Assess current and future information technology workforce needs across state agencies, identify skill gaps, and develop 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 provide existing employees with training or other opportunities to develop skills in emerging technologies and automation, ensuring that state agencies remain competitive and innovative.

(e) Develop strategies to recruit and retain information

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

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

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

282.0064 Information technology contract policy.—

(1) In coordination with the Department of Management Services, DIGIT 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 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 aligns 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 DIGIT on state term contract solicitations and invitations to negotiate related to information technology. Such coordination must include reviewing the solicitation specifications to verify compliance with enterprise architecture and cybersecurity standards, evaluating vendor responses under established criteria, answering vendor questions, and providing any other technical expertise necessary.

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

achieve the information technology policy.

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

282.318 Cybersecurity.—

(3) DIGIT ~~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 that comply with the latest 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. DIGIT ~~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. DIGIT ~~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 must ~~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) 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 and that is aligned with generally accepted technology best practices, including the National Institute for Standards and Technology Cybersecurity Framework.

3. Completing comprehensive risk assessments and cybersecurity audits, which may be completed by an independent third party ~~a private sector vendor~~, and submitting completed assessments and audits to DIGIT ~~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 DIGIT ~~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. If the event involves services housed or procured through the Northwest Regional Data Center, the state agency must also notify the Northwest Regional Data Center.

(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. If the event involves services housed or procured through the Northwest Regional Data Center, the state agency must also notify the Northwest Regional Data Center.

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)~~.

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

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

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.

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.~~

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

(e) In collaboration with the Cybercrime Office of the

Department of Law Enforcement, 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) Annually review the strategic and operational cybersecurity plans of state agencies.

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

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

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

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

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

(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 assess 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 an independent third party ~~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 an independent third party ~~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.

(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 DIGIT ~~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 must ~~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 DIGIT ~~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 must ~~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 DIGIT ~~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).

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) must ~~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) DIGIT ~~The department~~ shall adopt rules relating to cybersecurity and to administer this section.

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

282.3185 Local government cybersecurity.—

(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)(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)(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 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) 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 must ~~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 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 shall ~~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, 2022, the Florida Digital Service shall establish guidelines and processes for submitting an after-action report.~~

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

Section 19. 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 and shall meet or exceed the information technology standards specified in ss. 282.006 and 282.318 ~~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, 2026.~~

(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.~~

~~(e) 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 20. Section 282.2011, Florida Statutes, is created to read:

282.2011 Northwest Regional Data Center.—

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

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

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

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

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

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

new agreement;

3. Identify the scope of work;

4. Establish the services to be provided, the business standards that must be met for each service, the cost of each service, and the process by which the business standards for 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) For purposes of chapter 273, be the custodian of resources and equipment located in and operated, supported, and managed by the state data center.

(e) 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.

(f) 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.

(g) 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.

(h) 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.

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

(j) 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 for each state agency customer. The projections must include prior-year comparisons, identification of new services, and documentation of changes to billing methodologies or service cost allocation.

(k) 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 which increases any state agency customer's costs for that fiscal year.

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

(m) 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.

(n) Submit invoices to state agency customers.

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

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

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

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

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

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

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

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

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

2. A proposed governance structure to oversee the

implementation and operations of the repository.

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

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

5. Data security requirements for the repository.

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

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

(5) 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 pursuant to this chapter.

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

Statutes, is amended to read:

282.206 Cloud-first policy in state agencies.—

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

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

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

~~(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) 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.~~

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

~~(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.~~

~~(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.~~

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

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

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

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

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

~~c. Enhance the collection and coordination of treatment and~~

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

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

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

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

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

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

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

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

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

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

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

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

~~(5) 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 23. Section 287.0583, Florida Statutes, is created to read:

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

following:

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

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

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

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

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

287.0591 Information technology; vendor disqualification.—

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

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

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

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

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

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

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

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

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

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

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

(4)(a) An agency issuing a request for quote to purchase information technology commodities, information technology consultant services, or information technology staff augmentation contractual services from the state term contract which exceeds the CATEGORY FOUR threshold amount is subject to public records requirements pursuant to s. 287.057. Additionally, an agency shall publish:

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

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

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

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

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

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

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

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

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

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

Section 25. 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 26. 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 DIGIT ~~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 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 27. Section 282.604, Florida Statutes, is amended to read:

282.604 Adoption of rules.—DIGIT ~~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 28. 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 Division of Integrated Government Innovation and Technology within the Executive Office of the Governor ~~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 29. 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 Division of Integrated Government Innovation and Technology within the Executive Office of the Governor ~~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 30. 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 31. This act shall take effect January 5, 2027.