

Tab 1	SPB 7024 by AP; State Planning and Budgeting
--------------	---

Tab 2	SPB 7026 by AP; Information Technology
--------------	---

464614	A	S	FAV	AP, Harrell	btw L.375 - 376:	03/20 10:52 AM
208734	A	S	FAV	AP, Harrell	Delete L.710:	03/20 10:52 AM
784910	A	S	FAV	AP, Harrell	Delete L.1324 - 1459:	03/20 10:52 AM
867736	A	S	FAV	AP, Harrell	Delete L.2537 - 2901:	03/20 10:52 AM

Tab 3	SB 158 by Berman; Similar to H 00141 Coverage for Diagnostic and Supplemental Breast Examinations
--------------	--

The Florida Senate
COMMITTEE MEETING EXPANDED AGENDA

APPROPRIATIONS
Senator Hooper, Chair
Senator Rouson, Vice Chair

MEETING DATE: Thursday, March 20, 2025
TIME: 9:00 a.m.—12:00 noon
PLACE: *Toni Jennings Committee Room, 110 Senate Building*

MEMBERS: Senator Hooper, Chair; Senator Rouson, Vice Chair; Senators Berman, Brodeur, Burgess, Collins, DiCeglie, Fine, Garcia, Grall, Harrell, Martin, McClain, Pizzo, Polsky, Sharief, Smith, Trumbull, and Wright

TAB	BILL NO. and INTRODUCER	BILL DESCRIPTION and SENATE COMMITTEE ACTIONS	COMMITTEE ACTION
Consideration of proposed bill:			
1	SPB 7024	State Planning and Budgeting; Revising the purpose of long-range program plans; requiring that long-range program plans cover a specified timeframe and remain in effect until replaced or adjusted as provided by specified provisions; requiring state agencies, the judicial branch, and the Division of Administrative Hearings to submit legislative budget requests before a specified date in each odd-numbered year and by a specified date in each even-numbered year; requiring state agencies and the judicial branch to maintain performance measures, outcomes, and standards, etc.	Submitted and Reported Favorably as Committee Bill Yeas 18 Nays 0
Consideration of proposed bill:			
2	SPB 7026	Information Technology; Creating the Agency for State Systems and Enterprise Technology (ASSET); requiring that the Division of Elections comprehensive risk assessment comply with the risk assessment methodology developed by ASSET; requiring agencies and the judicial branch to include a cumulative inventory and a certain status report of specified projects with their legislative budget requests; revising the powers, duties, and functions of the Department of Management Services, through the Florida Digital Service, etc.	Submitted and Reported Favorably as Committee Bill Yeas 18 Nays 0
3	SB 158 Berman (Similar H 141)	Coverage for Diagnostic and Supplemental Breast Examinations; Prohibiting the state group insurance program from imposing any cost-sharing requirement upon an enrollee with respect to coverage for diagnostic breast examinations or supplemental breast examinations, etc.	Favorable Yeas 18 Nays 0
		AEG 03/05/2025 Favorable AP 03/20/2025 Favorable	

Other Related Meeting Documents

The Florida Senate
BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Appropriations

BILL: SB 7024
INTRODUCER: Appropriations Committee
SUBJECT: State Planning and Budgeting
DATE: March 20, 2025 REVISED: _____

ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1. Griffin	Sadberry		AP Submitted as Comm. Bill/FAV

I. Summary:

SB 7024 revises provisions within ch. 216, F.S., relating to the state budgeting and planning process, to clarify terminology, simplify the long-range program plan process, update the legislative budget request process, and remove obsolete provisions.

The bill does not impact state revenues or expenditures. **See Section V. Fiscal Impact Statement.**

The bill takes effect July 1, 2025.

II. Present Situation:

State Budgeting and Planning

Chapter 216, F.S., provides guidelines and requirements for the Executive Office of the Governor, state agencies, and the judicial branch for developing and submitting legislative budget requests and implementing legislative appropriations in accordance with s. 19, Art. III, of the Florida Constitution.

Long-Range Program Plans

The Florida Constitution requires general law to provide for a long-range state planning document. Section 216.013, F.S., requires state agencies and the judicial branch to develop long-range program plans to achieve state goals using an interagency planning process that includes the development of integrated agency program service outcomes.

The long-range program plans must provide the framework for the development of budget requests and identify, in part, the mission of the agency or judicial branch, the goals established to accomplish the mission, and the objectives developed to achieve state goals.¹ Each plan is

¹ Section 216.013(1), F.S.

required to cover a period of five fiscal years and must be revised annually. Each state agency and the judicial branch is required to post their long-range program plans on their websites no later than September 30th of each year.²

State agencies and the judicial branch were not required to develop or post an update to their plans going into planning and budgeting for the 2025-2026 fiscal year in light of the review that the Government Efficiency Task Force had undertaken.³

Performance Measures and Standards

Agencies and the judicial branch are required to maintain a comprehensive accountability system containing, at a minimum, a list of performance measures that are adopted by the Legislature. Agencies and the judicial branch must submit output and outcome measures and standards, as well as historical baseline performance data. The Legislature is authorized to create, amend, and delete performance measures and standards.⁴

Legislative Budget Requests

In accordance with s. 19, Art. III, of the Florida Constitution, s. 216.023, F.S., requires state agencies and the judicial branch to submit requests for the Legislature for the amounts of money such agency or branch believes will be needed in the performance of the functions that it is authorized, or which it is requesting authorization by law, to perform.⁵

Each state agency and the judicial branch is required to submit a final legislative budget request to the Legislature and the Governor in the form and manner prescribed by the budget instructions no later than October 15th of each year, unless an alternative date is agreed to be in the best interest of the state by the Governor and the chairs of the legislative appropriations committees.⁶

Agency Incentive and Savings Programs

Section 216.1815, F.S., authorizes agencies and the judicial branch to retain a portion of the savings produced by internally generated agency or judicial branch program efficiencies and cost reductions in order to provide an incentive for agencies and the judicial branch to re-engineer business processes and otherwise increase operating efficiency. To be eligible to retain funds, an agency or judicial branch must submit a plan and an associated request to amend its approved operating budget to the Legislative Budget Commission, which will determine the amount the agency or the judicial branch will be allowed to retain considering the actual savings projected for the current year budget and the annualized savings.⁷ Each agency or the judicial branch allowed to retain funds is required to submit in its next legislative budget request a schedule showing how it used such funds.⁸

² Section 216.013(4), F.S.

³ Section 216.013(7), F.S.

⁴ Section 216.1827, F.S.

⁵ Section 216.011(1)(cc), F.S.

⁶ Section 216.023.

⁷ Section 216.1815, F.S.

⁸ *Id.*

Activity-based Planning and Budgeting

Section 216.1826, F.S., requires agencies to work in consultation with the Executive Office of the Governor and the appropriation committees of the Legislature to identify and reach consensus on the appropriate services and activities for activity-based budgeting. Additionally, agencies or the judicial branch are required to examine approved performance measures and recommend any changes so that outcomes are clearly delineated for each service or program, as appropriate, and outputs are aligned with activities. Output measures should be capable of being used to generate a unit cost for each activity resulting in a true accounting of what the state should spend on each activity it provides and what the state should expect to accomplish with those funds.

Authorized Positions

The total number of authorized positions of a state agency or entity of the judicial branch may not exceed the total provided in the General Appropriations Act, unless otherwise expressly provided by law.⁹ If a state agency or entity of the judicial branch finds that the number of positions so provided is not sufficient to administer its authorized programs, it may file an application with the Executive Office of the Governor or the Chief Justice. If the Executive Office of the Governor or Chief Justice certifies that there are no authorized positions available for addition, deletion, or transfer within the agency and recommends an increase in the number of positions, the Governor or the Chief Justice may recommend an increase in the number of positions for the following reasons only:

- To implement or provide for continuing federal grants or changes in grants not previously anticipated.
- To meet emergencies pursuant to s. 252.36.
- To satisfy new federal regulations or changes therein.
- To take advantage of opportunities to reduce operating expenditures or to increase the revenues of the state or local government.
- To authorize positions that were not fixed by the Legislature through error in drafting the appropriations acts.¹⁰

Actions recommended by the Executive Office of the Governor or the Chief Justice are subject to the approval by the Legislative Budget Commission.¹¹

Historically, there has been an exception provided for the Department of Corrections in the bill implementing the General Appropriations Act.¹² For the 2024-2025 fiscal year, if the actual inmate population of the Department of Corrections exceeds the inmate population projections of the December 15, 2023, Criminal Justice Estimating Conference by 1 percent for 2 consecutive months or 2 percent for any month, the Executive Office of the Governor, with the approval of the Legislative Budget Commission, is required to immediately notify the Criminal Justice Estimating Conference, which shall convene as soon as possible to revise the estimates.

⁹ Section 216.262, F.S.

¹⁰ *Id.*

¹¹ *Id.*

¹² Chapter 2024-228, s. 28, L.O.F.

The Department of Corrections is then authorized to submit a budget amendment requesting the establishment of positions in excess of the number authorized by the Legislature and additional appropriations from unallocated general revenue sufficient to provide for essential staff, fixed capital improvements, and other resources to provide classification, security, food services, health services, and other variable expenses within the institutions to accommodate the estimated increase in the inmate population.¹³

Transfers of Appropriations

Funds provided in the General Appropriations Act or otherwise expressly provided by law are required to be expended only for the purpose for which appropriated. Appropriations may not be transferred between state agencies, or between a state agency and the judicial branch, unless specifically authorized by law.¹⁴

However, there are some exceptions provided in s. 216.292, F.S., provided the transfer is determined to be in the best interest of the state. Additionally, such authorized revisions must be consistent with the intent of the approved operating budget, must be consistent with legislative policy and intent, and may not conflict with specific spending policies specified in the General Appropriations Act.¹⁵

The transfer of appropriations funded from identical funding sources, except appropriations for fixed capital outlay, and the transfer of amounts included within the total original approved budget and plans of releases of appropriations as furnished pursuant to ss. 216.181 and 216.192, F.S., may be made by the head of each department or the Chief of the Supreme Court whenever it is deemed necessary by reason of changed conditions as follows:

- Between categories of appropriations within a budget entity, if no category of appropriation is increased or decreased by more than five percent of the original approved budget or \$250,000, whichever is greater, by all action taken under this subsection.
- Between budget entities within identical categories of appropriations, if no category of appropriation is increased or decreased by more than five percent of the original approved budget or \$250,000, whichever is greater, by all action taken under this subsection.¹⁶

However, any agency exceeding salary rate established pursuant to s. 216.181(8) on June 30th of any fiscal year is not authorized to make such transfers in the subsequent fiscal year.

Notice of proposed transfers must be provided to the Executive Office of the Governor and the chairs of the legislative appropriations committees at least three days prior to agency implementation, in order to provide an opportunity for review. The review shall be limited to ensuring that the transfer is in compliance with the requirements of this paragraph, but must ensure that transfers proposed pursuant to this paragraph comply with this chapter, maximize the use of available and appropriate trust funds, and are not contrary to legislative policy and intent.

¹³ Section 216.262(4), F.S.

¹⁴ *Id.*

¹⁵ Section 216.292, F.S.

¹⁶ Section 216.292(2), F.S.

The following transfers are authorized with the approval of the Executive Office of the Governor for the executive branch or the Chief Justice for the judicial branch, subject to the notice and objection provisions of s. 216.177, F.S.:

- The transfer of appropriations for operations from trust funds up to \$1 million.
- The transfer of positions between budget entities.¹⁷

The following transfers are authorized with the approval of the Legislative Budget Commission. Unless waived by the chair and vice chair of the commission, notice of such transfers must be provided 14 days before the commission meeting:

- The transfer of appropriations for operations from the General Revenue Fund in excess of \$1 million, but within a state agency or within the judicial branch, as recommended by the Executive Office of the Governor or the Chief Justice of the Supreme Court.
- The transfer of appropriations for operations from trust funds in excess of \$1 million, as recommended by the Executive Office of the Governor or the Chief Justice of the Supreme Court.
- The transfer of the portion of an appropriation for a named fixed capital outlay project found to be in excess of that needed to complete the project to another project for which there has been an appropriation in the same fiscal year from the same fund and within the same department where a deficiency is found to exist, at the request of the Executive Office of the Governor for state agencies or the Chief Justice of the Supreme Court for the judicial branch.
- The transfers necessary to accomplish the purposes of reorganization within state agencies or the judicial branch authorized by the Legislature when the necessary adjustments of appropriations and positions have not been provided in the General Appropriations Act.¹⁸

Government Efficiency Task Force

Article III, s. 19 of the Florida Constitution requires a Government Efficiency Task Force composed of members of the Legislature and representatives from the private and public sectors to develop recommendations for improving governmental operations and reducing costs. The task force is required to meet every four years and submit its work to the Joint Legislative Budget Commission, the Governor, and the Chief Justice of the Supreme Court.

In June 2024, the task force established a working group to study the Long-Range Program Plans. The working group reported the following recommendations and improvements:

- Improving flexibility through, creating a more dynamic process for revising plans based on new information, such as requiring agencies to update plans annually or bi-annually for more adaptable long-term strategic planning;
- Simplifying processes to reduce administrative demands and free up resources for service delivery, including a system for capturing lessons-learned and best practices from each planning cycle to aid with future planning cycles; and
- Shifting focus to outcomes, rather than outputs by requiring performance measures to focus on meaningful outcomes, rather than easily measured outputs.¹⁹

¹⁷ Section 216.292(3), F.S.

¹⁸ Section 216.292(4), F.S.

¹⁹ Florida Government Efficiency Task Force, *2024-2025 Final Recommendations*, at 3 (available at https://www.dms.myflorida.com/other_programs/government_efficiency_task_force).

III. Effect of Proposed Changes:

Section 1 amends s. 216.011, F.S., to clarify the definition of fixed capital outlay and specify that the definition does not include minor repairs or maintenance which may be appropriated in an expense, contracted services, or a special appropriations category. The bill also deletes the definitions for the terms “disincentives” and “incentives.”

Section 2 amends s. 216.013, F.S., to update the LRPP requirements. Pursuant to the bill, LRPPs must be submitted annually by each agency and the judicial branch by September 15 to the Legislative Budget Commission for approval, including any update on meeting their plans’ approved performance measure and any deviation from expected performance measures. An agency or the judicial branch that does not comply with the submission deadline and requirements will not be able to submit budget amendments or otherwise make changes to its budget until the agency or judicial branch has corrected the deficiency.

The LRPPs must include information about the implementation status of any law enacted in the previous legislative session. The status must be provided until all provisions of the law are fully implemented. For the purposes of initial implementation, an agency must provide information on laws enacted in the 2023 and 2024 regular session that have provision not fully implemented.

The implementation status information must include:

- Actions or steps taken to implement the law, including but not limited to:
 - Administrative rules for proposed implementation.
 - Procurements required.
 - Contracts executed to assist the agency in implementation.
 - Contracts executed to implement or administer the law.
 - Programs started, offices established, or other organizational administrative changes made, including personnel changes.
 - Federal waivers requested.
- The status of any required appointments and timing of board, commission, or related public meetings.
- A description of the agency programs, outputs, and activities implemented or changed related to the law.
- All expenditures made that were directly related to the implementation.
- Any provisions remaining to be implemented.
- A description of any impediment or delay in the implementation, including, but not limited to, challenges of administrative rules or identification of any policy issue that needs to be resolved by the Legislature to ensure timely and effective implementation.
- Information related to any litigation related to the law which is not previously provided.
- Performance measures developed and the specific data identified, including data on enrollments, participants, loans, and other data elements of programs, outputs, and activities.

Additionally, the bill requires each LRPP to be posted on the agency or judicial branch website no later than September 30th of each year.

Section 3 amends s. 216.023, F.S., to clarify that Legislative Budget Requests (LBRs) are due no later than September 15th of each odd-numbered year and no later than October 15th of each even-numbered year.

The bill further amends s. 216.023, F.S., to repeal the requirements for the LRPP and LBR Unit Cost Summary exercise.

The bill also updates the Governor's Office of Policy and Budget title from the current Planning and Budgeting title.

Section 4 amends s. 216.163, F.S., to remove the requirement that the Executive Office of the Governor review and submit recommendations for executive agencies regarding incentives and disincentives for agency performance.

Section 5 amends s. 216.177, F.S., to remove the authorization for the Legislature to annually specify any incentives and disincentives for agencies operating programs under performance-based budgets.

Section 6 amends s. 216.181, F.S., to conform a cross-reference.

Section 7 repeals s. 216.1815, F.S., relating to the agency incentive and savings program.

Section 8 repeals s. 216.1826, F.S., relating to activity-based planning and budgeting.

Section 9 amends s. 216.1827, F.S., to provide standardization of agency performance measures, outcomes, and standards.

Pursuant to the bill, each state agency and the judicial branch shall adopt the new, standardized, performance measures, outcomes, and standards. These new reporting requirements include:

- Administrative costs as a percentage of total agency costs, including salaries and benefits and excluding fixed capital outlay.
- The percentage of vacant positions filled within 180 days after becoming vacant.
- Total dollar amount of salary increases awarded, delineated by the subtotal dollar amount associated with increases specifically authorized in the General Appropriations Act or other law and the amount awarded without specific legislative authorization.
- Percentage of corrective actions taken within 6 months after receipt of audit findings and management letters issued to resolve such findings or letters from financial and operational audits conducted pursuant to s. 11.45, F.S.
- Private attorney service costs dollar amounts by case and as a percentage of total agency legal costs, legal costs paid to the Attorney General's office by case and as a percentage of total agency legal costs, and total agency legal costs as a percentage of total agency budget.
- Total dollar 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 agency procurements through request for proposal, invitation to negotiate, invitation to bid, single source, and emergency purchases.

- If applicable, the number of complete applications received and the average number of days to complete a permit, a licensure, a registration, or a certification process, from the date of the receipt of initial application to final agency action, for each permit, license, registration, or certification issued by the agency or judicial branch.
- If applicable, the total number of required inspections, total number of inspections completed, and percentage of required inspections completed.
- If applicable, average number of calendar days to award and contract for noncompetitive projects or grant programs for state or federal funds from the date of receipt of funds by the agency or receipt of budget authority, whichever is later.

The bill further provides that, in addition to the standard performance measures, outcomes, and standards required by subsection (2), each agency and the judicial branch shall develop and adopt at least five additional performance measures, outcomes, and standards. Additional performance measures, outcomes, and standards must include key state agency or judicial branch functions.

When developing the additional performance measures, outcomes, and standards, each state agency and the judicial branch shall take all of the following into consideration:

- The mission of the agency or judicial branch, state goals and objectives, and statutory policy.
- Programs, outputs, and activities that are key agency or judicial branch functions.
- Selection of data elements that best and most accurately measure progress toward state goals and objectives, including facilitating analysis of any deviation from expected performance.

Additionally, the bill requires each agency and the judicial branch to maintain the justification for each performance measure, outcome, or standard, as well as the source of data to be used.

The bill adds language to require LRPPs to provide:

- Information regarding measurement of the performance measures, including how the data is collected, baseline data, the methodology used for measurement, the reason for the measurement, and the validity and reliability of the measurement.
- Data for the previous five years related to the performance measures, outcomes, and standards and an explanation of deviation from expected performance.

The bill makes several revisions to the submission, approval, and amendment process for agency LRPPs. Under the provisions of the bill:

- Each state agency and the judicial branch shall submit performance measures, outcomes, and standards, including any information required under this section, to the Office of Program Policy Analysis and Government Accountability (OPPAGA).
- The performance measures, outcomes, and standards, including any amendments thereto, for each state agency and the judicial branch are to be adopted by the LBC.
- At least 30 days before the scheduled annual legislative session, a state agency or the Chief Justice of the Supreme Court may submit requests to delete or amend performance measures, outcomes, and standards. Such deletion, amendment, or addition is subject to review and approval by the LBC.

- State agencies and the judicial branch have 30 days after the effective date of the General Appropriations Act, or other enacted legislation, to propose adjustments to their performance measures, outcomes, and standards for review and approval by the LBC.
- Any new state agency created by the legislature is required to establish initial performance measures, outcomes, and standards subject to review and approval by the LBC.
- Each state agency and the judicial branch shall submit new performance measures, outcomes, and standards, including the information required by this section to the LBC by December 1, 2025. This paragraph will expire on December 31, 2026.

Section 10 amends s. 216.262, F.S., to authorize the Department of Corrections to request additional positions through the LBC if the inmate population exceeds the most recently adopted forecast by the Criminal Justice Estimating Conference for specified percentages and timeframes.

Section 11 amends s. 216.292, F.S., to allow the Executive Office of the Governor to transfer funds between agencies for the purpose of implementing statewide distributions for risk management insurance, human resource services, and data processing services. These transfers and adjustments are subject to the notice, review, and objection procedures of s. 216.177, F.S.

The bill further requires the review of agency transfer budget amendments to ensure that the transfers comply with the requirements of chg. 216, F.S., maximize the use of available and appropriate trust funds, and are not contrary to legislative policy and intent.

Section 12 amends s. 20.055, F.S., to remove the provision that agency inspectors general are required to assess the reliability and validity of performance measures and standards and make recommendations for improvement before submission.

Section 16 amends s. 420.0003, F.S., to allow the Florida Housing Finance Corporation to independently develop a long-range plan rather than developing an LRPP in coordination with the Department of Commerce.

Section 17 amends s. 420.511, F.S., to remove the provision that the Secretary of Commerce, or their designee, serves as the Florida Housing Finance Corporation's representative to achieve planning coordination and integration with the department.

Sections 13-15 and 18-21 amend ss. 121.021, 121.051, 186.021, 489.145, 985.619, 1002.37, and 402.56, F.S., respectively, to make technical and conforming changes.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

None.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 216.011, 216.013, 216.023, 216.163, 216.177, 216.181, 216.1827, 216.262, 216.292, 20.055, 121.021, 121.051, 186.021, 420.0003, 420.511, 985.619, and 1002.37.

This bill repeals the following sections of the Florida Statutes: 216.1815 and 216.1826.

IX. Additional Information:

A. Committee Substitute – Statement of Changes:

(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.

This Senate Bill Analysis does not reflect the intent or official position of the bill's introducer or the Florida Senate.

FOR CONSIDERATION By the Committee on Appropriations

576-02446-25

20257024pb

1 A bill to be entitled
 2 An act relating to state planning and budgeting;
 3 reenacting and amending s. 216.011, F.S.; deleting the
 4 definitions of the terms "disincentive" and
 5 "incentive"; revising the definition of the term
 6 "fixed capital outlay"; amending s. 216.013, F.S.;
 7 revising the purpose of long-range program plans;
 8 requiring that such plans be based on statutorily
 9 established policies and driven by priorities and
 10 outcomes to achieve certain goals, objectives, and
 11 policies; requiring that such plans provide the
 12 framework for development of legislative budget
 13 requests; requiring that such plans identify specified
 14 performance measures, trends and conditions relevant
 15 to the performance measures and state goals, and
 16 agency and judicial programs that implement
 17 statutorily established policy; requiring that such
 18 plans include certain information regarding the
 19 implementation status of enacted laws; requiring that
 20 such information also include laws enacted in
 21 specified years; requiring that the implementation
 22 status include specified information; requiring that
 23 long-range program plans cover a specified timeframe
 24 and remain in effect until replaced or adjusted as
 25 provided by specified provisions; deleting a
 26 requirement that written notice be provided to the
 27 Governor and Legislature upon the publishing of such
 28 plans on the agency or judicial branch website;
 29 requiring state agencies and the judicial branch

Page 1 of 36

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

576-02446-25

20257024pb

30 annually, by a specified date, to submit their long-
 31 range program plans to the Legislative Budget
 32 Commission for approval; providing that if a state
 33 agency or the judicial branch receives a certain
 34 notification of failure to comply, such agency or the
 35 judicial branch is prohibited from submitting
 36 amendments to or otherwise making changes to its
 37 approved budget for certain expenditures until
 38 compliance is achieved; deleting obsolete language;
 39 amending s. 216.023, F.S.; requiring state agencies,
 40 the judicial branch, and the Division of
 41 Administrative Hearings to submit legislative budget
 42 requests before a specified date in each odd-numbered
 43 year and by a specified date in each even-numbered
 44 year; deleting provisions relating to total
 45 accountability measures and reductions in allocations;
 46 making a technical change; amending ss. 216.163,
 47 216.177, and 216.181, F.S.; conforming provisions to
 48 changes made by the act; repealing ss. 216.1815 and
 49 216.1826, F.S., relating to the agency incentive and
 50 savings program and activity-based planning and
 51 budgeting, respectively; amending s. 216.1827, F.S.;
 52 requiring state agencies and the judicial branch to
 53 maintain performance measures, outcomes, and
 54 standards; requiring state agencies and the judicial
 55 branch to adopt specified and applicable performance
 56 measures, outcomes, and standards; requiring state
 57 agencies and the judicial branch to develop and adopt
 58 a certain number of specified performance measures,

Page 2 of 36

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

576-02446-25

20257024pb

59 outcomes, and standards; requiring state agencies and
 60 the judicial branch to consider specified factors when
 61 developing such additional performance measures,
 62 outcomes, and standards; requiring state agencies to
 63 maintain justifications for and sources of data to be
 64 used for each performance measure adopted; requiring
 65 that the long-range program plans contain performance
 66 measures in specified forms, manner, and timeframes;
 67 requiring that such plans provide specified
 68 information and data; requiring state agencies and the
 69 judicial branch to submit performance measures,
 70 outcomes, standards, and certain information to the
 71 Office of Program Policy Analysis and Government
 72 Accountability upon request; requiring that certain
 73 performance measures be adopted by the Legislative
 74 Budget Commission; authorizing the submission of
 75 requests to delete or amend performance measures,
 76 outcomes, and standards to the Legislative Budget
 77 Commission; requiring that such request include the
 78 justification for the deletion, amendment, or
 79 addition; providing that such deletions, amendments,
 80 or additions are subject to review and approval by the
 81 Legislative Budget Commission; requiring state
 82 agencies and the judicial branch to make appropriate
 83 adjustments to their performance measures, outcomes,
 84 and standards to be consistent with certain enacted
 85 legislation; providing that state agencies and the
 86 judicial branch have a specified timeframe to make
 87 such adjustments; deleting obsolete language;

Page 3 of 36

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

576-02446-25

20257024pb

88 requiring new state agencies created by the
 89 Legislature to establish initial performance measures,
 90 outcomes, and standards that are subject to review and
 91 approval by the Legislative Budget Commission;
 92 requiring state agencies and the judicial branch to
 93 submit to the Legislative Budget Commission new
 94 performance measures and specified information by a
 95 specified date; providing for the scheduled repeal of
 96 such provision; amending s. 216.262, F.S.; providing
 97 that if the actual inmate population of the Department
 98 of Corrections exceeds inmate population projections
 99 of the most recently adopted forecast published by the
 100 Criminal Justice Estimating Conference for the current
 101 fiscal year by specified percentages, the Executive
 102 Office of the Governor shall immediately notify such
 103 estimating conference to convene and revise the
 104 estimates; abrogating the scheduled repeal of such
 105 provisions; amending s. 216.292, F.S.; prohibiting
 106 appropriations from being transferred between state
 107 agencies unless specifically authorized by the General
 108 Appropriations Act or as otherwise provided by law;
 109 authorizing the Executive Office of the Governor to
 110 transfer funds within and between state agencies for a
 111 specified purpose; providing that such transfers and
 112 adjustments are subject to certain notice, review, and
 113 objections; deleting obsolete language; abrogating the
 114 scheduled repeal of a provision; amending s. 20.055,
 115 F.S.; conforming provisions to changes made by the
 116 act; amending ss. 121.021 and 121.051, F.S.;

Page 4 of 36

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

576-02446-25

20257024pb

117 conforming cross-references; amending s. 186.021,
 118 F.S.; conforming provisions to changes made by the
 119 act; amending s. 420.0003, F.S.; revising that a
 120 certain long-range plan is from the Florida Housing
 121 Finance Corporation and not from the Department of
 122 Commerce; conforming provisions to changes made by the
 123 act; amending s. 420.511, F.S.; revising references to
 124 "long-range program plan" as "long-range plan";
 125 deleting a requirement that such plan be developed in
 126 coordination with the Department of Commerce; deleting
 127 a provision relating to the Secretary of Commerce, or
 128 his or her designee, serving as the Florida Housing
 129 Finance Corporation's liaison for a specified purpose;
 130 amending ss. 489.145, 985.619 and 1002.37, F.S.;

131 conforming cross-references; reenacting s.
 132 402.56(5)(d), F.S., relating to the duty of the
 133 Children and Youth Cabinet to design and implement a
 134 long-range program plan, to incorporate the amendment
 135 made to s. 216.013, F.S., in a reference thereto;
 136 providing an effective date.

137
 138 Be It Enacted by the Legislature of the State of Florida:

139
 140 Section 1. Paragraphs (n), (r), and (v) of subsection (1)
 141 of section 216.011, Florida Statutes, are amended, and paragraph
 142 (ee) of that subsection is reenacted, to read:

143 216.011 Definitions.—

144 (1) For the purpose of fiscal affairs of the state,
 145 appropriations acts, legislative budgets, and approved budgets,

Page 5 of 36

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

576-02446-25

20257024pb

146 each of the following terms has the meaning indicated:

147 ~~(n) "Disincentive" means a sanction as described in s.~~
 148 ~~216.163.~~

149 (q) ~~(r)~~ "Fixed capital outlay" means the appropriation
 150 category used to fund real property (land, buildings, including
 151 appurtenances, fixtures and fixed equipment, structures, etc.),
 152 including additions, replacements, major repairs, and
 153 renovations to real property which materially extend its useful
 154 life or materially improve or change its functional use and
 155 including furniture and equipment necessary to furnish and
 156 operate a new or improved facility, when appropriated by the
 157 Legislature in the fixed capital outlay appropriation category.
 158 The term does not include a minor repair or maintenance that
 159 does not materially extend the useful life or materially improve
 160 or change the functional use of a facility, which may be
 161 appropriated in an expense, contracted services, or special
 162 appropriation category.

163 ~~(v) "Incentive" means a mechanism, as described in s.~~
 164 ~~216.163, for recognizing the achievement of performance~~
 165 ~~standards or for motivating performance that exceeds performance~~
 166 ~~standards.~~

167 (cc) ~~(ee)~~ "Long-range program plan" means a plan developed
 168 pursuant to s. 216.013.

169 Section 2. Section 216.013, Florida Statutes, is amended to
 170 read:

171 216.013 Long-range program plans ~~plan~~.—State agencies and
 172 the judicial branch shall develop long-range program plans to
 173 achieve state goals and objectives using an interagency planning
 174 process ~~that includes the development of integrated agency~~

Page 6 of 36

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

576-02446-25

20257024pb

175 ~~program service outcomes.~~ The plans must shall be ~~policy~~ based
 176 on statutorily established policies; ~~priority driven by~~
 177 priorities and outcomes to achieve state goals, objectives, and
 178 policies; ~~accountable;~~ and developed through careful
 179 examination and justification of all agency and judicial branch
 180 programs and activities.

181 (1) Long-range program plans must ~~shall~~ provide the
 182 framework for the development of legislative budget requests.

183 (2) Long-range program plans must ~~and shall~~ identify ~~or~~
 184 update:

185 (a) The mission of the agency or judicial branch.

186 (b) The performance measures required pursuant to s.
 187 216.1827 ~~goals established to accomplish the mission.~~

188 (c) ~~The objectives developed to achieve state goals.~~

189 ~~(d)~~ The trends and conditions relevant to the mission, the
 190 performance measures, and the state goals, ~~and objectives.~~

191 (d)(e) The state agency or judicial branch programs that
 192 will be used to implement statutorily established ~~state~~ policy
 193 and achieve state goals and objectives.

194 ~~(f)~~ ~~The program outcomes and standards to measure progress~~
 195 ~~toward program objectives.~~

196 ~~(g)~~ ~~Information regarding performance measurement, which~~
 197 ~~includes, but is not limited to, how data is collected, the~~
 198 ~~methodology used to measure a performance indicator, the~~
 199 ~~validity and reliability of a measure, the appropriateness of a~~
 200 ~~measure, and whether, in the case of agencies, the agency~~
 201 ~~inspector general has assessed the reliability and validity of~~
 202 ~~agency performance measures, pursuant to s. 20.055(2).~~

203 ~~(h)~~ ~~Legislatively approved output and outcome performance~~

576-02446-25

20257024pb

204 ~~measures.~~ Each performance measure must identify the associated
 205 activity contributing to the measure from those identified in
 206 ~~accordance with s. 216.023(4)(b).~~

207 ~~(i)~~ ~~Performance standards for each performance measure and~~
 208 ~~justification for the standards and the sources of data to be~~
 209 ~~used for measurement. Performance standards must include~~
 210 ~~standards for each affected activity and be expressed in terms~~
 211 ~~of the associated unit of activity.~~

212 ~~(j)~~ ~~Prior-year performance data on approved performance~~
 213 ~~measures and an explanation of deviation from expected~~
 214 ~~performance. Performance data must be assessed for reliability~~
 215 ~~in accordance with s. 20.055.~~

216 ~~(k)~~ ~~Proposed performance incentives and disincentives.~~

217 (3) (a) 1. Long-range program plans must include information
 218 about the implementation status of any law enacted in the
 219 previous legislative session. The implementation status must be
 220 provided until all provisions of the law related to the agency
 221 have been fully implemented.

222 2. For purposes of initial implementation of this
 223 subsection, in addition to laws enacted pursuant to the 2025
 224 Regular Session, an agency must also provide information on
 225 recently enacted laws for the 2023 and 2024 Regular Sessions
 226 that have provisions not fully implemented. This subparagraph
 227 expires on June 30, 2026.

228 (b) Implementation status information must include, at a
 229 minimum, all of the following:

230 1. Actions or steps taken to implement the law, and actions
 231 or steps planned for implementation, including, but not limited
 232 to, all of the following, as applicable:

576-02446-25

20257024pb

233 a. Administrative rules proposed for implementation.
 234 b. Procurements required.
 235 c. Contracts executed to assist the agency in
 236 implementation.
 237 d. Contracts executed to implement or administer the law.
 238 e. Programs started, offices established, or other
 239 organizational administrative changes made, including personnel
 240 changes.
 241 f. Federal waivers requested.
 242 2. The status of any required appointments and all
 243 scheduled board, commission, or related public meetings.
 244 3. A description of the agency programs, outputs, and
 245 activities implemented or changed related to the law.
 246 4. All expenditures made that were directly related to the
 247 implementation.
 248 5. Any provisions remaining to be implemented.
 249 6. A description of any impediment or delay in the
 250 implementation, including, but not limited to, challenges of
 251 administrative rules or identification of any policy issue that
 252 needs to be resolved by the Legislature to ensure timely and
 253 effective implementation.
 254 7. Information related to any litigation related to the law
 255 which is not provided under subparagraph 6.
 256 8. Any performance measure developed and the specific data
 257 identified, including data regarding enrollments, participants,
 258 loans, and other data elements of programs, outputs, and
 259 activities.
 260 (4)(2) Each Long-range program plans must plan shall cover
 261 a period of 5 fiscal years, be revised annually, and remain in

Page 9 of 36

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

576-02446-25

20257024pb

262 effect until replaced or adjusted as provided in this section
 263 ~~revised.~~
 264 (5)(3) Long-range program plans or revisions must shall be
 265 presented by state agencies and the judicial branch in a form,
 266 manner, and timeframe prescribed in written instructions
 267 prepared by the Executive Office of the Governor in consultation
 268 with the chairs of the legislative appropriations committees.
 269 (6)(4) Each state executive agency and the judicial branch
 270 shall post their long-range program plans on their Internet
 271 websites not later than September 30 30th of each year, and
 272 provide written notice to the Governor and the Legislature that
 273 the plans have been posted.
 274 (7)(5) Each state agency The state agencies and the
 275 judicial branch shall make appropriate adjustments to their
 276 long-range program plans, excluding adjustments to performance
 277 measures, outcomes, and standards, to be consistent with the
 278 appropriations in the General Appropriations Act, and
 279 legislation implementing the General Appropriations Act, or
 280 other enacted legislation. Agencies and the judicial branch have
 281 30 days subsequent to the effective date of the General
 282 Appropriations Act and implementing legislation to make
 283 adjustments to their plans as posted on their Internet websites.
 284 (8) Annually, no later than September 15, each state agency
 285 and the judicial branch shall submit their long-range program
 286 plans to the Legislative Budget Commission for approval,
 287 including any update on meeting their plans' approved
 288 performance measures and any deviation from expected performance
 289 measures.
 290 (9) If the chairs of the legislative appropriations

Page 10 of 36

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

576-02446-25

20257024pb

291 committees notify a state agency or the judicial branch that the
 292 agency or the judicial branch has failed to comply with this
 293 section or s. 216.1827, the agency or the judicial branch may
 294 not submit amendments or otherwise make changes to its approved
 295 budget for operations and fixed capital outlay pursuant to s.
 296 216.181 until the agency or the judicial branch has corrected
 297 its deficiency.

298 ~~(10)(6)~~ Long-range program plans developed pursuant to this
 299 chapter are not rules and, therefore, are not subject to the
 300 provisions of chapter 120.

301 ~~(7) Notwithstanding the provisions of this section, each~~
 302 ~~state executive agency and the judicial branch are not required~~
 303 ~~to develop or post a long-range program plan by September 30,~~
 304 ~~2024, for the 2025-2026 fiscal year, except in circumstances~~
 305 ~~outlined in any updated written instructions prepared by the~~
 306 ~~Executive Office of the Governor in consultation with the chairs~~
 307 ~~of the legislative appropriations committees. This subsection~~
 308 ~~expires July 1, 2025.~~

309 Section 3. Subsections (1), (2), (4), and (10) of section
 310 216.023, Florida Statutes, are amended to read:

311 216.023 Legislative budget requests to be furnished to
 312 Legislature by agencies.—

313 (1) The head of each state agency, except as provided in
 314 subsection (2), shall submit a final legislative budget request
 315 to the Legislature and to the Governor, as chief budget officer
 316 of the state, in the form and manner prescribed in the budget
 317 instructions and at such time as specified by the Executive
 318 Office of the Governor, based on the agency's independent
 319 judgment of its needs. However, a state agency must ~~may not~~

Page 11 of 36

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

576-02446-25

20257024pb

320 submit its complete legislative budget request, including all
 321 supporting forms and schedules required by this chapter, no
 322 later than September 15 of each odd-numbered year and no later
 323 than October 15 of each even-numbered year unless an alternative
 324 date is agreed to be in the best interest of the state by the
 325 Governor and the chairs of the legislative appropriations
 326 committees.

327 (2) The judicial branch and the Division of Administrative
 328 Hearings shall submit their complete legislative budget requests
 329 directly to the Legislature with a copy to the Governor, as
 330 chief budget officer of the state, in the form and manner as
 331 prescribed in the budget instructions. However, the complete
 332 legislative budget requests, including all supporting forms and
 333 schedules required by this chapter, must ~~shall~~ be submitted no
 334 later than September 15 of each odd-numbered year and no later
 335 than October 15 of each even-numbered year unless an alternative
 336 date is agreed to be in the best interest of the state by the
 337 Governor and the chairs of the legislative appropriations
 338 committees.

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

341 ~~(a)1-~~ The constitutional or statutory authority for a
 342 program, a brief purpose statement, and approved program
 343 components.

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

348 ~~(c)3-~~ Details on trust funds and fees.

Page 12 of 36

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

576-02446-25

20257024pb

349 (d)4- The total number of positions (authorized, fixed, and
350 requested).

351 (e)5- An issue narrative describing and justifying changes
352 in amounts and positions requested for current and proposed
353 programs for the next fiscal year.

354 (f)6- Information resource requests.

355 (g)7- Supporting information, including applicable cost-
356 benefit analyses, business case analyses, performance
357 contracting procedures, service comparisons, and impacts on
358 performance standards for any request to outsource or privatize
359 agency functions. The cost-benefit and business case analyses
360 must include an assessment of the impact on each affected
361 activity ~~from those identified in accordance with paragraph (b)-~~
362 ~~Performance standards must include standards for each affected~~
363 ~~activity and be expressed in terms of the associated unit of~~
364 ~~activity.~~

365 (h)8- An evaluation of major outsourcing and privatization
366 initiatives undertaken during the last 5 fiscal years having
367 aggregate expenditures exceeding \$10 million during the term of
368 the contract. The evaluation must include an assessment of
369 contractor performance, a comparison of anticipated service
370 levels to actual service levels, and a comparison of estimated
371 savings to actual savings achieved. Consolidated reports issued
372 by the Department of Management Services may be used to satisfy
373 this requirement.

374 (i)9- Supporting information for any proposed consolidated
375 financing of deferred-payment commodity contracts including
376 guaranteed energy performance savings contracts. Supporting
377 information must also include narrative describing and

576-02446-25

20257024pb

378 justifying the need, baseline for current costs, estimated cost
379 savings, projected equipment purchases, estimated contract
380 costs, and return on investment calculation.

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

394 ~~(b) It is the intent of the Legislature that total~~
395 ~~accountability measures, including unit cost data, serve not~~
396 ~~only as a budgeting tool but also as a policymaking tool and an~~
397 ~~accountability tool. Therefore, each state agency and the~~
398 ~~judicial branch must submit a summary of information for the~~
399 ~~preceding year in accordance with the legislative budget~~
400 ~~instructions. Each summary must provide a one-page overview and~~
401 ~~must contain:~~

- 402 ~~1. The final budget for the agency and the judicial branch.~~
- 403 ~~2. Total funds from the General Appropriations Act.~~
- 404 ~~3. Adjustments to the General Appropriations Act.~~
- 405 ~~4. The line item listings of all activities.~~
- 406 ~~5. The number of activity units performed or accomplished.~~

576-02446-25

20257024pb

407 ~~6. Total expenditures for each activity, including amounts~~
 408 ~~paid to contractors and subordinate entities. Expenditures~~
 409 ~~related to administrative activities not aligned with output~~
 410 ~~measures must consistently be allocated to activities with~~
 411 ~~output measures prior to computing unit costs.~~

412 ~~7. The cost per unit for each activity, including the costs~~
 413 ~~allocated to contractors and subordinate entities.~~

414 ~~8. The total amount of reversions and pass-through~~
 415 ~~expenditures omitted from unit cost calculations.~~

416
 417 At the regular session immediately following the submission of
 418 the agency unit cost summary, the Legislature shall reduce in
 419 the General Appropriations Act for the ensuing fiscal year, by
 420 an amount equal to at least 10 percent of the allocation for the
 421 fiscal year preceding the current fiscal year, the funding of
 422 each state agency that fails to submit the report required under
 423 this paragraph.

424 (10) The legislative budget request from each agency and
 425 from the judicial branch shall be reviewed by the Legislature.
 426 The review may allow for the opportunity to have information or
 427 testimony by the agency, the judicial branch, the Auditor
 428 General, the Office of Program Policy Analysis and Government
 429 Accountability, the Governor's Office of Policy and Budget
 430 Planning and Budgeting, and the public regarding the proper
 431 level of funding for the agency in order to carry out its
 432 mission.

433 Section 4. Subsection (4) of section 216.163, Florida
 434 Statutes, is amended to read:

435 216.163 Governor's recommended budget; form and content;

Page 15 of 36

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

576-02446-25

20257024pb

436 declaration of collective bargaining impasses.-

437 ~~(4) The Executive Office of the Governor shall review the~~
 438 ~~findings of the Office of Program Policy Analysis and Government~~
 439 ~~Accountability, to the extent they are available, request any~~
 440 ~~reports or additional analyses as necessary, and submit a~~
 441 ~~recommendation for executive agencies, which may include a~~
 442 ~~recommendation regarding incentives or disincentives for agency~~
 443 ~~performance. Incentives or disincentives may apply to all or~~
 444 ~~part of a state agency. The Chief Justice shall review the~~
 445 ~~findings of the Office of Program Policy Analysis and Government~~
 446 ~~Accountability regarding judicial branch performance and make~~
 447 ~~appropriate recommendations for the judicial branch.~~

448 ~~(a) Incentives may include, but are not limited to:~~

449 ~~1. Additional flexibility in budget management, such as,~~
 450 ~~but not limited to, the use of lump sums or special categories;~~
 451 ~~consolidation of budget entities or program components;~~
 452 ~~consolidation of appropriation categories; and increased agency~~
 453 ~~transfer authority between appropriation categories or budget~~
 454 ~~entities.~~

455 ~~2. Additional flexibility in salary rate and position~~
 456 ~~management.~~

457 ~~3. Retention of up to 50 percent of all unencumbered~~
 458 ~~balances of appropriations as of June 30, or undisbursed~~
 459 ~~balances as of December 31, excluding special categories and~~
 460 ~~grants and aids, which may be used for nonrecurring purposes~~
 461 ~~including, but not limited to, lump-sum bonuses, employee~~
 462 ~~training, or productivity enhancements, including technology and~~
 463 ~~other improvements.~~

464 ~~4. Additional funds to be used for, but not limited to,~~

Page 16 of 36

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

576-02446-25

20257024pb

465 ~~lump-sum bonuses, employee training, or productivity~~
 466 ~~enhancements, including technology and other improvements.~~

467 ~~5. Additional funds provided pursuant to law to be released~~
 468 ~~to an agency quarterly or incrementally contingent upon the~~
 469 ~~accomplishment of units of output or outcome specified in the~~
 470 ~~General Appropriations Act.~~

471 ~~(b) Disincentives may include, but are not limited to:~~

472 ~~1. Mandatory quarterly reports to the Executive Office of~~
 473 ~~the Governor and the Legislature on the agency's progress in~~
 474 ~~meeting performance standards.~~

475 ~~2. Mandatory quarterly appearances before the Legislature,~~
 476 ~~the Governor, or the Governor and Cabinet to report on the~~
 477 ~~agency's progress in meeting performance standards.~~

478 ~~3. Elimination or restructuring of the program, which may~~
 479 ~~include, but not be limited to, transfer of the program or~~
 480 ~~outsourcing all or a portion of the program.~~

481 ~~4. Reduction of total positions for a program.~~

482 ~~5. Restriction on or reduction of the spending authority~~
 483 ~~provided in s. 216.292(2)(b).~~

484 ~~6. Reduction of managerial salaries.~~

485 Section 5. Subsection (3) of section 216.177, Florida
 486 Statutes, is amended to read:

487 216.177 Appropriations acts, statement of intent,
 488 violation, notice, review and objection procedures.—

489 ~~(3) The Legislature may annually specify any incentives and~~
 490 ~~disincentives for agencies operating programs under performance-~~
 491 ~~based budgets pursuant to this chapter in the General~~
 492 ~~Appropriations Act or legislation implementing the General~~
 493 ~~Appropriations Act.~~

Page 17 of 36

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

576-02446-25

20257024pb

494 Section 6. Paragraph (b) of subsection (10) of section
 495 216.181, Florida Statutes, is amended to read:

496 216.181 Approved budgets for operations and fixed capital
 497 outlay.—

498 (10)

499 (b) Lump-sum salary bonuses may be provided only if
 500 specifically appropriated or provided pursuant to s. 110.1245 ~~or~~
 501 ~~s. 216.1815.~~

502 Section 7. Section 216.1815, Florida Statutes, is repealed.

503 Section 8. Section 216.1826, Florida Statutes, is repealed.

504 Section 9. Section 216.1827, Florida Statutes, is amended
 505 to read:

506 216.1827 Requirements for performance measures, outcomes,
 507 and standards.—

508 (1) Each state agency ~~Agencies~~ and the judicial branch
 509 shall maintain a ~~comprehensive performance accountability system~~
 510 ~~containing, at a minimum, a list of performance measures,~~
 511 outcomes, and standards as required by that are adopted by the
 512 ~~Legislature and subsequently amended pursuant to this section.~~

513 (2) Each state agency and the judicial branch shall adopt
 514 the following performance measures, outcomes, and standards:

515 (a) Administrative costs as a percentage of total agency
 516 costs, including salaries and benefits and excluding fixed
 517 capital outlay.

518 (b) Percentage of vacant positions filled within 180 days
 519 after becoming vacant.

520 (c) Total dollar amount of salary increases awarded,
 521 delineated by the subtotal dollar amount of the increases
 522 specifically authorized in the General Appropriations Act or

Page 18 of 36

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

576-02446-25

20257024pb

523 other law and the subtotal dollar amount of the increases
 524 awarded without specific legislative authorization.

525 (d) Percentage of corrective actions taken within 6 months
 526 after receipt of audit findings and management letters issued to
 527 resolve such findings or letters from financial and operational
 528 audits conducted pursuant to s. 11.45.

529 (e) Private attorney service costs dollar amounts by case
 530 and as a percentage of total agency legal costs, legal costs
 531 paid to the Attorney General's office by case and as a
 532 percentage of total agency legal costs, and total agency legal
 533 costs as a percentage of total agency budget.

534 (f) Total dollar amount of expenditures by state term
 535 contract as defined in s. 287.012, contracts procured using
 536 alternative purchasing methods as authorized pursuant to s.
 537 287.042(16), and agency procurements through request for
 538 proposal, invitation to negotiate, invitation to bid, single
 539 source, and emergency purchases.

540 (g) If applicable, the number of complete applications
 541 received and the average number of days to complete a permit, a
 542 licensure, a registration, or a certification process, from the
 543 date of the receipt of initial application to final agency
 544 action, for each permit, license, registration, or certification
 545 issued by the agency or judicial branch.

546 (h) If applicable, the total number of required
 547 inspections, total number of inspections completed, and
 548 percentage of required inspections completed.

549 (i) If applicable, average number of calendar days to award
 550 and contract for noncompetitive projects or grant programs for
 551 state or federal funds from the date of receipt of funds by the

576-02446-25

20257024pb

552 agency or receipt of budget authority, whichever is later.

553 (3) In addition to the performance measures, outcomes, and
 554 standards required by subsection (2), each agency and the
 555 judicial branch shall develop and adopt at least five additional
 556 performance measures, outcomes, and standards. Additional
 557 performance measures, outcomes, and standards must include key
 558 state agency or judicial branch functions. When developing the
 559 additional performance measures, outcomes, and standards, each
 560 state agency and the judicial branch shall take all of the
 561 following into consideration:

562 (a) The mission of the agency or judicial branch, state
 563 goals and objectives, and statutory policy.

564 (b) Programs, outputs, and activities that are key agency
 565 or judicial branch functions.

566 (c) Selection of data elements that best and most
 567 accurately measure progress toward state goals and objectives,
 568 including facilitating analysis of any deviation from expected
 569 performance.

570 (4) Each state agency and the judicial branch shall
 571 maintain the justification for each performance measure,
 572 outcome, or standard, and the sources of data to be used.

573 (5)-(2)-(a) Each state agency ~~Agencies~~ and the judicial
 574 branch shall submit long-range program plans with performance
 575 measures in the form, manner, and timeframe ~~output and outcome~~
 576 ~~measures and standards, as well as historical baseline and~~
 577 ~~performance data~~ pursuant to s. 216.013. The long-range program
 578 plan must provide:

579 (a) Information regarding measurement of the performance
 580 measures, including how the data is collected, baseline data,

576-02446-25

20257024pb

581 the methodology used for measurement, the reason for the
 582 measurement, and the validity and reliability of the
 583 measurement.

584 (b) Data for the previous 5 years related to the
 585 performance measures, outcomes, and standards and an explanation
 586 of deviation from expected performance.

587 (6) Each state agency ~~Agencies~~ and the judicial branch
 588 shall also submit performance data, measures, outcomes, and
 589 standards, including any information required by this section,
 590 to the Office of Program Policy Analysis and Government
 591 Accountability upon request for review of the adequacy of the
 592 legislatively approved measures and standards.

593 (7) For each state agency and the judicial branch,
 594 performance measures, outcomes, and standards, including any
 595 amendments thereto, must be adopted by the Legislative Budget
 596 Commission.

597 ~~(3)~~ (a) At least 30 days before the scheduled annual
 598 legislative session, a state an agency or the Chief Justice of
 599 the Supreme Court may submit requests to delete or amend its
 600 existing approved performance measures, outcomes, and standards
 601 or activities, including alignment of activities to performance
 602 measures, or submit requests to create additional performance
 603 measures, outcomes, and standards or activities to the
 604 Legislature Executive Office of the Governor for review and
 605 approval. The request must shall document the justification for
 606 the change and ensure that the revision, deletion, amendment, or
 607 addition is consistent with legislative intent. Such deletion,
 608 amendment, or addition is subject to review and approval by the
 609 Legislative Budget Commission Revisions or deletions to or

Page 21 of 36

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

576-02446-25

20257024pb

610 ~~additions of performance measures and standards approved by the~~
 611 ~~Executive Office of the Governor are subject to the review and~~
 612 ~~objection procedure set forth in s. 216.177.~~

613 (b) Each state agency and the judicial branch shall make
 614 appropriate adjustments to their performance measures, outcomes,
 615 and standards to be consistent with the appropriations in the
 616 General Appropriations Act, legislation implementing the General
 617 Appropriations Act, or other enacted legislation. State agencies
 618 and the judicial branch have 30 days after the effective date of
 619 the General Appropriations Act or other enacted legislation to
 620 propose adjustments to their plans for review and approval by
 621 the Legislative Budget Commission The Chief Justice of the
 622 Supreme Court may submit deletions or amendments of the judicial
 623 branch's existing approved performance measures and standards or
 624 may submit additional performance measures and standards to the
 625 Legislature accompanied with justification for the change and
 626 ensure that the revision, deletion, or addition is consistent
 627 with legislative intent. Revisions or deletions to, or additions
 628 of performance measures and standards submitted by the Chief
 629 Justice of the Supreme Court are subject to the review and
 630 objection procedure set forth in s. 216.177.

631 ~~(4) (a) The Legislature may create, amend, and delete~~
 632 ~~performance measures and standards. The Legislature may confer~~
 633 ~~with the Executive Office of the Governor for state agencies and~~
 634 ~~the Chief Justice of the Supreme Court for the judicial branch~~
 635 ~~prior to any such action.~~

636 ~~(b) The Legislature may require state agencies to submit~~
 637 ~~requests for revisions, additions, or deletions to approved~~
 638 ~~performance measures and standards to the Executive Office of~~

Page 22 of 36

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

576-02446-25

20257024pb

639 the Governor for review and approval, subject to the review and
640 objection procedure set forth in s. 216.177.

641 (c) ~~The Legislature may require the judicial branch to~~
642 ~~submit revisions, additions, or deletions to approved~~
643 ~~performance measures and standards to the Legislature, subject~~
644 ~~to the review and objection procedure set forth in s. 216.177.~~

645 (d) Any new state agency created by the Legislature shall
646 establish is subject to the initial performance measures,
647 outcomes, and standards thereof, subject to review and approval
648 by the Legislative Budget Commission established by the
649 Legislature. The Legislature may require state agencies and the
650 judicial branch to provide any information necessary to create
651 initial performance measures and standards.

652 (d) Each state agency and the judicial branch shall submit
653 new performance measures, outcomes, and standards, including the
654 information required by this section, to the Legislative Budget
655 Commission by December 1, 2025. This paragraph expires on
656 December 31, 2026.

657 Section 10. Subsection (4) of section 216.262, Florida
658 Statutes, is amended to read:

659 216.262 Authorized positions.—

660 (4) Notwithstanding the provisions of this chapter relating
661 to increasing the number of authorized positions, ~~and for the~~
662 ~~2024-2025 fiscal year only~~, if the actual inmate population of
663 the Department of Corrections in the current fiscal year exceeds
664 the inmate population projections of the most recently adopted
665 forecast published by the December 15, 2023, Criminal Justice
666 Estimating Conference for the current fiscal year by 1 percent
667 for 2 consecutive months or 2 percent for any month, the

Page 23 of 36

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

576-02446-25

20257024pb

668 Executive Office of the Governor, with the approval of the
669 Legislative Budget Commission, shall immediately notify the
670 Criminal Justice Estimating Conference, which shall convene as
671 soon as possible to revise the estimates. The Department of
672 Corrections may then submit a budget amendment requesting the
673 establishment of positions in excess of the number authorized by
674 the Legislature and additional appropriations from unallocated
675 general revenue sufficient to provide for essential staff, fixed
676 capital improvements, and other resources to provide
677 classification, security, food services, health services, and
678 other variable expenses within the institutions to accommodate
679 the estimated increase in the inmate population. All actions
680 taken pursuant to this subsection are subject to review and
681 approval by the Legislative Budget Commission. ~~This subsection~~
682 ~~expires July 1, 2025.~~

683 Section 11. Present paragraph (b) of subsection (1) of
684 section 216.292, Florida Statutes, is redesignated as paragraph
685 (c), a new paragraph (b) is added to that subsection, and
686 paragraph (a) of subsection (1) and subsection (2) of that
687 section are amended, to read:

688 216.292 Appropriations nontransferable; exceptions.—

689 (1) (a) Funds provided in the General Appropriations Act or
690 as otherwise expressly provided by law shall be expended only
691 for the purpose for which appropriated, except that such moneys
692 may be transferred as provided in this section when it is
693 determined to be in the best interest of the state.
694 Appropriations for fixed capital outlay may not be expended for
695 any other purpose. Appropriations may not be transferred between
696 state agencies, or between a state agency and the judicial

Page 24 of 36

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

576-02446-25

20257024pb

697 branch, unless specifically authorized by law or specifically
 698 authorized in the General Appropriations Act.

699 (b) The Executive Office of the Governor may transfer funds
 700 within and between state agencies for the sole purpose of
 701 implementing statewide distributions for risk management
 702 insurance, human resource services, and data processing
 703 services. Transfers and adjustments are subject to the notice,
 704 review, and objection procedures of s. 216.177.

705 (2) The following transfers are authorized to be made by
 706 the head of each department or the Chief Justice of the Supreme
 707 Court whenever it is deemed necessary by reason of changed
 708 conditions:

709 (a) The transfer of appropriations funded from identical
 710 funding sources, except appropriations for fixed capital outlay,
 711 and the transfer of amounts included within the total original
 712 approved budget and plans of releases of appropriations as
 713 furnished pursuant to ss. 216.181 and 216.192, as follows:

714 1. Between categories of appropriations within a budget
 715 entity, if no category of appropriation is increased or
 716 decreased by more than 5 percent of the original approved budget
 717 or \$250,000, whichever is greater, by all action taken under
 718 this subsection.

719 2. Between budget entities within identical categories of
 720 appropriations, if no category of appropriation is increased or
 721 decreased by more than 5 percent of the original approved budget
 722 or \$250,000, whichever is greater, by all action taken under
 723 this subsection.

724 3. Any agency exceeding salary rate established pursuant to
 725 s. 216.181(8) on June 30th of any fiscal year may shall not be

Page 25 of 36

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

576-02446-25

20257024pb

726 ~~authorized to~~ make transfers pursuant to subparagraphs 1. and 2.
 727 in the subsequent fiscal year.

728 4. Notice of proposed transfers under subparagraphs 1. and
 729 2. shall be provided to the Executive Office of the Governor and
 730 the chairs of the legislative appropriations committees at least
 731 3 days prior to agency implementation in order to provide an
 732 opportunity for review. The review shall be limited to ensuring
 733 that the transfer is in compliance with the requirements of this
 734 paragraph.

735 5. ~~For the 2024-2025 fiscal year,~~ The review shall ensure
 736 that transfers proposed pursuant to this paragraph comply with
 737 this chapter, maximize the use of available and appropriate
 738 trust funds, and are not contrary to legislative policy and
 739 intent. ~~This subparagraph expires July 1, 2025.~~

740 (b) After providing notice at least 5 working days prior to
 741 implementation:

742 1. The transfer of funds within programs identified in the
 743 General Appropriations Act from identical funding sources
 744 between the following appropriation categories without
 745 limitation so long as such a transfer does not result in an
 746 increase, to the total recurring general revenue or trust fund
 747 cost of the agency or entity of the judicial branch in the
 748 subsequent fiscal year: other personal services, expenses,
 749 operating capital outlay, food products, state attorney and
 750 public defender operations, data processing services, operating
 751 and maintenance of patrol vehicles, overtime payments, salary
 752 incentive payments, compensation to retired judges, law
 753 libraries, and juror and witness payments.

754 2. The transfer of funds and positions from identical

Page 26 of 36

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

576-02446-25

20257024pb

755 funding sources between salaries and benefits appropriation
756 categories within programs identified in the General
757 Appropriations Act. Such transfers must be consistent with
758 legislative policy and intent and may not adversely affect
759 achievement of approved performance outcomes or outputs in any
760 program.

761 (c) The transfer of funds appropriated to accounts
762 established for disbursement purposes upon release of such
763 appropriation upon request of a department and approval by the
764 Chief Financial Officer. Such transfer may only be made to the
765 same appropriation category and the same funding source from
766 which the funds are transferred.

767 Section 12. Paragraphs (a) and (b) of subsection (2) of
768 section 20.055, Florida Statutes, are amended to read:

769 20.055 Agency inspectors general.—

770 (2) An office of inspector general is established in each
771 state agency to provide a central point for coordination of and
772 responsibility for activities that promote accountability,
773 integrity, and efficiency in government. It is the duty and
774 responsibility of each inspector general, with respect to the
775 state agency in which the office is established, to:

776 (a) Advise in the development of performance measures,
777 outcomes, standards, and procedures for the evaluation of state
778 agency programs.

779 ~~(b) Assess the reliability and validity of the information~~
780 ~~provided by the state agency on performance measures and~~
781 ~~standards, and make recommendations for improvement, if~~
782 ~~necessary, before submission of such information pursuant to s.~~
783 ~~216.1827.~~

Page 27 of 36

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

576-02446-25

20257024pb

784 Section 13. Paragraph (a) of subsection (52) and paragraph
785 (a) of subsection (53) of section 121.021, Florida Statutes, are
786 amended to read:

787 121.021 Definitions.—The following words and phrases as
788 used in this chapter have the respective meanings set forth
789 unless a different meaning is plainly required by the context:

790 (52) "Regularly established position" means:

791 (a) With respect to a state employer, a position that is
792 authorized and established pursuant to law and is compensated
793 from a salaries and benefits appropriation pursuant to s.
794 216.011(1)(pp) ~~s. 216.011(1)(pp)~~, or an established position
795 that is authorized pursuant to s. 216.262(1)(a) and (b) and is
796 compensated from a salaries account as provided in s.
797 216.011(qq) ~~s. 216.011(1)(ss)~~.

798 (53) "Temporary position" means:

799 (a) With respect to a state employer, a position that is
800 compensated from an other personal services (OPS) account as
801 provided in s. 216.011(1)(hh) ~~s. 216.011(1)(jj)~~.

802 Section 14. Subsection (8) of section 121.051, Florida
803 Statutes, is amended to read:

804 121.051 Participation in the system.—

805 (8) DIVISION OF REHABILITATION AND LIQUIDATION EMPLOYEES
806 MEMBERSHIP.—Effective July 1, 1994, the regular receivership
807 employees of the Division of Rehabilitation and Liquidation of
808 the Department of Financial Services who are assigned to
809 established positions and are subject to established rules and
810 regulations regarding discipline, pay, classification, and time
811 and attendance are hereby declared to be state employees within
812 the meaning of this chapter and shall be compulsory members in

Page 28 of 36

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

576-02446-25

20257024pb

813 compliance with this chapter, the provisions of s.
 814 216.011(1)(hh)2. ~~s. 216.011(1)(jj)2.~~, notwithstanding.
 815 Employment performed before July 1, 1994, as such a receivership
 816 employee may be claimed as creditable retirement service upon
 817 payment by the employee or employer of contributions required in
 818 s. 121.081(1), as applicable for the period claimed.

819 Section 15. Section 186.021, Florida Statutes, is amended
 820 to read:

821 186.021 Long-range program plans.—Pursuant to s. 216.013,
 822 each state agency shall develop a long-range program plan ~~on an~~
 823 ~~annual basis~~. The plan must shall provide the framework and
 824 context for designing and interpreting the agency budget
 825 request. The plan must will be developed through careful
 826 examination and justification of agency functions ~~and their~~
 827 ~~associated costs~~. An agency shall use the long-range program
 828 plan It shall be used by the agency to implement the state's
 829 goals and objectives. The agency shall also develop performance
 830 measures, outcomes, and standards to measure programs, outputs,
 831 Indicators shall be developed to measure service and activity
 832 performance.

833 Section 16. Paragraph (b) of subsection (3) of section
 834 420.0003, Florida Statutes, is amended to read:

835 420.0003 State housing strategy.—

836 (3) IMPLEMENTATION.—The state, in carrying out the strategy
 837 articulated in this section, shall have the following duties:

838 (b) The long-range ~~program~~ plan of the corporation
 839 ~~department~~ must include specific performance measures, goals,
 840 and objectives, ~~and strategies~~ that implement the housing
 841 policies in this section.

Page 29 of 36

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

576-02446-25

20257024pb

842 Section 17. Section 420.511, Florida Statutes, is amended
 843 to read:

844 420.511 Strategic business plan; long-range ~~program~~ plan;
 845 annual report; audited financial statements.—

846 (1) The corporation shall develop a strategic business plan
 847 for the provision of affordable housing for the state. The plan
 848 must be consistent with the long-range ~~program~~ plan prepared
 849 pursuant to subsection (2) and must shall contain performance
 850 measures and specific performance targets for the following:

851 (a) The ability of low-income and moderate-income
 852 Floridians to access housing that is decent and affordable.

853 (b) The continued availability and affordability of housing
 854 financed by the corporation to target populations.

855 (c) The availability of affordable financing programs,
 856 including equity and debt products, and programs that reduce
 857 gaps in conventional financing in order to increase individual
 858 access to housing and stimulate private production of affordable
 859 housing.

860 (d) The establishment and maintenance of efficiencies in
 861 the delivery of affordable housing.

862 (e) Such other measures as directed by the corporation's
 863 board of directors.

864 (2) The corporation, ~~in coordination with the department,~~
 865 shall annually develop a long-range ~~program~~ plan for the
 866 provision of affordable housing in this state as required
 867 pursuant to chapter 186. In part, the plan must include
 868 provisions that maximize the abilities of the corporation to
 869 implement the state housing strategy established under s.
 870 420.0003, to respond to federal housing initiatives, and to

Page 30 of 36

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

576-02446-25

20257024pb

871 develop programs in a manner that is more responsive to the
 872 needs of public and private partners. The plan ~~must shall~~ be
 873 developed on a schedule consistent with that established by s.
 874 186.021. ~~For purposes of this section, the Secretary of Commerce~~
 875 ~~or his or her designee shall serve as the corporation's~~
 876 ~~representative to achieve a coordinated and integrated planning~~
 877 ~~relationship with the department.~~

878 (3) The corporation shall submit to the Governor and the
 879 presiding officers of each house of the Legislature, within 6
 880 months after the end of its fiscal year, a complete and detailed
 881 report setting forth the corporation's state and federal program
 882 accomplishments using the most recent available data. The report
 883 must include, but is not limited to:

884 (a) The following tenant characteristics in the existing
 885 rental units financed through corporation-administered programs:

886 1. The number of households served, delineated by income,
 887 race, ethnicity, and age of the head of household.

888 2. The number of households served in large, medium, and
 889 small counties as described in s. 420.5087(1) and the extent to
 890 which geographic distribution has been achieved in accordance
 891 with s. 420.5087.

892 3. The number of farmworker and commercial fishing worker
 893 households served.

894 4. The number of homeless households served.

895 5. The number of special needs households served.

896 6. By county, the average rent charged based on unit size.

897 (b) The number of rental units to which resources have been
 898 allocated in the last fiscal year, including income and
 899 demographic restrictions.

576-02446-25

20257024pb

900 (c) The estimated average cost of producing units under
 901 each rental or homeownership unit financed under each program in
 902 the last fiscal year.

903 (d) By county, the average sales price of homeownership
 904 units financed in the last fiscal year.

905 (e) The number of households served by homeownership
 906 programs in the last fiscal year, including the income, race,
 907 ethnicity, and age of the homeowner of each household.

908 (f) The percentage of homeownership loans that are in
 909 foreclosure.

910 (g) The percentage of properties in the corporation's
 911 rental portfolio which have an occupancy rate below 90 percent.

912 (h) The amount of economic stimulus created by the
 913 affordable housing finance programs administered by the
 914 corporation for the most recent year available.

915 (i) For the State Apartment Incentive Loan Program (SAIL),
 916 a comprehensive list of all closed loans outstanding at the end
 917 of the most recent fiscal year, including, but not limited to,
 918 development name, city, county, developer, set-aside type, set-
 919 aside percentage, affordability term, total number of units,
 920 number of set-aside units, lien position, original loan amount,
 921 loan maturity date, loan balance at close of year, status of
 922 loan, rate of interest, and interest paid.

923 (j) For the Florida Affordable Housing Guarantee Program, a
 924 list of all guaranteed loans through the close of the most
 925 recent fiscal year, including, but not limited to, development
 926 name, city, county, developer, total number of units, issuer of
 927 the bonds, loan maturity date, participation in the United
 928 States Department of Housing and Urban Development Risk-Sharing

576-02446-25 20257024pb

929 Program, original guarantee amount, guarantee amount at the
 930 close of the fiscal year, status of guaranteed loans, and total
 931 outstanding Florida Housing Finance Corporation Affordable
 932 Housing Guarantee Program revenue bonds at the close of the most
 933 recent fiscal year.

934 (k) Any other information the corporation deems
 935 appropriate.

936 (4) Within 6 months after the end of its fiscal year, the
 937 corporation shall submit audited financial statements, prepared
 938 in accordance with generally accepted accounting principles,
 939 which include all assets, liabilities, revenues, and expenses of
 940 the corporation, and a list of all bonds outstanding at the end
 941 of its fiscal year. The audit must be conducted by an
 942 independent certified public accountant, performed in accordance
 943 with generally accepted auditing standards and government
 944 auditing standards, and incorporate all reports, including
 945 compliance reports, as required by such auditing standards.

946 (5) The Auditor General shall conduct an operational audit
 947 of the accounts and records of the corporation and provide a
 948 written report on the audit to the President of the Senate and
 949 the Speaker of the House of Representatives by December 1, 2016.

950 Section 18. Paragraph (a) of subsection (6) of section
 951 489.145, Florida Statutes, is amended to read:

952 489.145 Guaranteed energy, water, and wastewater
 953 performance savings contracting.—

954 (6) PROGRAM ADMINISTRATION AND CONTRACT REVIEW.—The
 955 Department of Management Services, with the assistance of the
 956 Office of the Chief Financial Officer, shall, within available
 957 resources, provide technical content assistance to state

576-02446-25 20257024pb

958 agencies contracting for energy, water, and wastewater
 959 efficiency and conservation measures and engage in other
 960 activities considered appropriate by the department for
 961 promoting and facilitating guaranteed energy, water, and
 962 wastewater performance contracting by state agencies. The
 963 Department of Management Services shall review the investment-
 964 grade audit for each proposed project and certify that the cost
 965 savings are appropriate and sufficient for the term of the
 966 contract. The Office of the Chief Financial Officer, with the
 967 assistance of the Department of Management Services, shall,
 968 within available resources, develop model contractual and
 969 related documents for use by state agencies. Before entering
 970 into a guaranteed energy, water, and wastewater performance
 971 savings contract, a contract or lease for third-party financing,
 972 or any combination of such contracts, a state agency shall
 973 submit such proposed contract or lease to the Office of the
 974 Chief Financial Officer for review and approval. The Office of
 975 the Chief Financial Officer shall complete its review and
 976 approval within 10 business days after receiving the proposed
 977 contract or lease. A proposed contract or lease with a state
 978 agency must include the following:

979 (a) Supporting information required by s. 216.023(4)(i) ~~or~~
 980 ~~216.023(4)(a)9.~~ in ss. 287.063(5) and 287.064(11). For contracts
 981 approved under this section, the criteria may, at a minimum,
 982 include the specification of a benchmark cost of capital and
 983 minimum real rate of return on energy, water, or wastewater
 984 savings against which proposals shall be evaluated.

985
 986 The Office of the Chief Financial Officer shall not approve any

576-02446-25 20257024pb

987 contract submitted under this section from a state agency that
988 does not meet the requirements of this section.

989 Section 19. Paragraph (c) of subsection (5) of section
990 985.619, Florida Statutes, is amended to read:

991 985.619 Florida Scholars Academy.—

992 (5) FUNDING.—

993 (c) The fiscal year for the Florida Scholars Academy is the
994 fiscal year of the state as defined in s. 216.011(1)(n) ~~s.~~
995 ~~216.011(1)(c)~~.

996 Section 20. Paragraph (a) of subsection (2) of section
997 1002.37, Florida Statutes, is amended to read:

998 1002.37 The Florida Virtual School.—

999 (2) The Florida Virtual School shall be governed by a board
1000 of trustees comprised of seven members appointed by the Governor
1001 to 4-year staggered terms. The board of trustees shall be a
1002 public agency entitled to sovereign immunity pursuant to s.
1003 768.28, and board members shall be public officers who shall
1004 bear fiduciary responsibility for the Florida Virtual School.
1005 The board of trustees shall have the following powers and
1006 duties:

1007 (a)1. The board of trustees shall meet at least 4 times
1008 each year, upon the call of the chair, or at the request of a
1009 majority of the membership.

1010 2. The fiscal year for the Florida Virtual School shall be
1011 the state fiscal year as provided in s. 216.011(1)(p) ~~s.~~
1012 ~~216.011(1)(g)~~.

1013
1014 The Governor shall designate the initial chair of the board of
1015 trustees to serve a term of 4 years. Members of the board of

576-02446-25 20257024pb

1016 trustees shall serve without compensation, but may be reimbursed
1017 for per diem and travel expenses pursuant to s. 112.061. The
1018 board of trustees shall be a body corporate with all the powers
1019 of a body corporate and such authority as is needed for the
1020 proper operation and improvement of the Florida Virtual School.
1021 The board of trustees is specifically authorized to adopt rules,
1022 policies, and procedures, consistent with law and rules of the
1023 State Board of Education related to governance, personnel,
1024 budget and finance, administration, programs, curriculum and
1025 instruction, travel and purchasing, technology, students,
1026 contracts and grants, and property as necessary for optimal,
1027 efficient operation of the Florida Virtual School. Tangible
1028 personal property owned by the board of trustees shall be
1029 subject to the provisions of chapter 273.

1030 Section 21. For the purpose of incorporating the amendment
1031 made by this act to section 216.013, Florida Statutes, in a
1032 reference thereto, paragraph (d) of subsection (5) of section
1033 402.56, Florida Statutes, is reenacted to read:

1034 402.56 Children's cabinet; organization; responsibilities;
1035 annual report.—

1036 (5) DUTIES AND RESPONSIBILITIES.—The Children and Youth
1037 Cabinet shall:

1038 (d) Design and implement actions that will promote
1039 collaboration, creativity, increased efficiency, information
1040 sharing, and improved service delivery between and within state
1041 governmental organizations that provide services for children
1042 and youth and their families. In particular, the efforts shall
1043 include the long-range planning process mandated by s. 216.013.

1044 Section 22. This act shall take effect July 1, 2025.

The Florida Senate
BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Appropriations

BILL: SB 7026

INTRODUCER: Appropriations Committee

SUBJECT: Information Technology

DATE: March 24, 2025

REVISED: _____

ANALYST

Hunter/Davis

STAFF DIRECTOR

Sadberry

REFERENCE

ACTION

AP Submitted as Comm. Bill/FAV

I. Summary:

SB 7026 establishes the Agency for State Systems and Enterprise Technology (ASSET) as a Cabinet agency, with the majority of its operations becoming effective on July 1, 2026. The state Chief Information Officer (CIO) will serve as the ASSET's executive director, nominated by a CIO selection committee, appointed by a majority Cabinet vote, and confirmed by the Senate, with removal also requiring a majority Cabinet vote.

Beginning in July 2026, all executive state agencies will be subject to the ASSET's published standards and rules, removing existing exemptions for the Department of Agriculture and Consumer Services, Department of Financial Services, and Department of Legal Affairs. A state CIO policy workgroup will review the ASSET's structure, functions, and powers, submitting recommendations for changes to the Legislature by December 1, 2025.

The ASSET will be organized into divisions and bureaus specializing in areas such as agency operations, data, security, business analysis, quality assurance, project management, contract management, procurement, and workforce development. Subject matter experts within the ASSET will form consulting teams dedicated to specific state agency program areas, including health and human services, education, government operations, justice, agriculture, and transportation. These teams will provide state agency assistance and feedback to the ASSET for developing guidelines and standards, with workgroups of state agency experts advising the ASSET on enterprise architecture.

The ASSET will absorb non-operational functions of the Florida Digital Service (FLDS), adding responsibilities such as master data management, legacy system needs assessments, information technology (IT) expenditure tracking, and an IT test lab for evaluating software and services. The ASSET will also develop career training programs for the state's IT workforce. The FLDS will be abolished on June 30, 2026, with its remaining responsibilities limited to agency needs assessments, transitioning cybersecurity services, and reporting cybersecurity incidents in Fiscal Year 2025-2026.

The bill also mandates biennial cybersecurity risk assessments for state agencies, including vulnerability and penetration testing, with leadership acknowledgment of the risks. It eliminates the Cybersecurity Advisory Council, removes outdated data center management language from law, requires the Northwest Regional Data Center (NWRDC) to meet or exceed the standards established by the ASSET, and requires the NWRDC to provide projected state data center costs to the Executive Office of the Governor's Office of Policy and Budget and the Legislature by November 15 each year.

The bill has significant fiscal impact on state expenditures. **See Part V., Fiscal Impact Statement.**

Except as otherwise provided, the bill takes effect July 1, 2025.

II. Present Situation:

Over the past decade, the landscape of information technology governance and management has evolved significantly, with state governments across the U.S. striving to modernize their Information Technology (IT) infrastructure and enhance digital services. The need for sound management and governance has been exacerbated by the rapidly growing concern of cybersecurity. The cyberattacks are growing in frequency and severity. Cybercrime is expected to inflict \$10.5 trillion worth of damage globally in 2025.¹ The United States is often a target of cyberattacks, including attacks on critical infrastructure, and has been a target of more significant cyberattacks² over the last 14 years than any other country.³ The Colonial Pipeline is an example of critical infrastructure that was attacked, disrupting what is arguably the nation's most important fuel conduit.⁴

Ransomware is a type of cybersecurity incident where malware⁵ that is designed to encrypt files on a device renders the files and the systems that rely on them unusable. In other words, critical information is no longer accessible. During a ransomware attack, malicious actors demand a ransom in exchange for regained access through decryption. If the ransom is not paid, the ransomware actors will often threaten to sell or leak the data or authentication information. Even if the ransom is paid, there is no guarantee that the bad actor will follow through with decryption.

¹ Cybercrime Magazine, *Cybercrime to Cost the World \$10.5 Trillion Annually By 2025*, <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/> (last visited March 12, 2025).

² "Significant cyber-attacks" are defined as cyberattacks on a country's government agencies, defense and high-tech companies, or economic crimes with losses equating to more than a million dollars. FRA Conferences, *Study: U.S. Largest Target for Significant Cyber-Attacks*, <https://www.fraconferences.com/insights-articles/compliance/study-us-largest-target-for-significant-cyber-attacks/#:~:text=The%20United%20States%20has%20been%20on%20the%20receiving,article%20is%20from%20FRA%27s%20sister%20company%2C%20Compliance%20Week> (last visited March 12, 2025).

³ *Id.*

⁴ S&P Global, *Pipeline operators must start reporting cyberattacks to government: TSA orders*, https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/electric-power/052721-pipeline-operators-must-start-reporting-cyberattacks-to-government-tsa-orders?utm_campaign=corporatepro&utm_medium=contentdigest&utm_source=esgmay2021 (last visited March 12, 2025).

⁵ "Malware" means hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. NIST, Computer Security Resource Center Glossary, *malware*, <https://csrc.nist.gov/glossary/term/malware> (last visited March 12, 2025).

In recent years, ransomware incidents have become increasingly prevalent among the nation's state, local, tribal, and territorial government entities and critical infrastructure organizations.⁶ For example, Tallahassee Memorial Hospital was hit by a ransomware attack February 2023, and the hospital's systems were forced to shut down, impacting many local residents in need of medical care.⁷

Information Technology and Cybersecurity Management

The Department of Management Services (DMS) oversees information technology (IT)⁸ governance and security for the executive branch in Florida.⁹ The Florida Digital Service (FLDS) is housed within the DMS and was established in 2020 to replace the Division of State Technology.¹⁰ The FLDS works under the DMS to implement policies for information technology and cybersecurity for state agencies.¹¹

The head of the FLDS is appointed by the Secretary of Management Services¹² and serves as the state chief information officer (CIO).¹³ The CIO must have at least five years of experience in the development of IT system strategic planning and IT policy and, preferably, have leadership-level experience in the design, development, and deployment of interoperable software and data solutions.¹⁴ The FLDS must propose innovative solutions that securely modernize state government, including technology and information services, to achieve value through digital transformation and interoperability, and to fully support Florida's cloud first policy.¹⁵

The DMS, through the FLDS, has the following powers, duties, and functions:

- Develop IT policy for the management of the state's IT resources;
- Develop an enterprise architecture;
- Establish project management and oversight standards with which state agencies must comply when implementing IT projects;
- Perform project oversight on all state agency IT projects that have a total cost of \$10 million or more and that are funded in the General Appropriations Act or any other law; and

⁶ Cybersecurity and Infrastructure Agency, *Ransomware 101*, <https://www.cisa.gov/stopransomware/ransomware-101> (last visited March 12, 2025).

⁷ Tallahassee Democrat, *TMH says it has taken 'major step' toward restoration after cybersecurity incident* (February 15, 2023) <https://www.tallahassee.com/story/news/local/2023/02/14/tmh-update-hospital-has-taken-major-step-toward-restoration/69904510007/> (last visited March 12, 2025).

⁸ The term "information technology" means equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form. Section 282.0041(20), F.S.

⁹ *See* s. 20.22, F.S.

¹⁰ Chapter 2020-161, L.O.F.

¹¹ *See* s. 20.22(2)(b), F.S.

¹² The Secretary of Management Services serves as the head of the DMS and is appointed by the Governor, subject to confirmation by the Senate. Section 20.22(1), F.S.

¹³ Section 282.0051(2)(a), F.S.

¹⁴ *Id.*

¹⁵ Section 282.0051 (1), F.S.

- Identify opportunities for standardization and consolidation of IT services that support interoperability, Florida’s cloud first policy, and business functions and operations that are common across state agencies.¹⁶

Information Technology Security Act

In 2021, the Legislature passed the IT Security Act,¹⁷ which requires the DMS and the state agency¹⁸ heads to meet certain requirements in order to enhance the IT security of state agencies. Specifically, the IT Security Act provides that the DMS is responsible for establishing standards and processes consistent with accepted best practices for IT security,¹⁹ including cybersecurity, and adopting rules that help agencies safeguard their data, information, and IT resources to ensure availability, confidentiality, integrity, and to mitigate risks.²⁰ In addition, the DMS must:

- Designate a state chief information security officer to oversee state IT security;
- Develop, and annually update, a statewide IT security strategic plan;
- Develop and publish an IT security governance framework for use by state agencies;
- Collaborate with the Cybercrime Office within the Florida Department of Law Enforcement (FDLE) to provide training; and
- Annually review the strategic and operational IT security plans of executive branch agencies.²¹

State Cybersecurity Act

In 2022, the Legislature passed the State Cybersecurity Act,²² which requires the DMS and the heads of the state agencies²³ to meet certain requirements to enhance the cybersecurity²⁴ of the state agencies.

The DMS through the FLDS is tasked with completing the following:

- Establishing standards for assessing agency cybersecurity risks;

¹⁶ *Id.*

¹⁷ Section 282.318, F.S.

¹⁸ The term “state agency” means any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include university boards of trustees or state universities. Section 282.0041(33), F.S. For purposes of the IT Security Act, the term includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services. Section 282.318(2), F.S.

¹⁹ The term “information technology security” means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of data, information, and information technology resources. Section 282.0041(22), F.S.

²⁰ Section 292.318(3), F.S.

²¹ *Id.*

²² Section 282.318, F.S.

²³ For purposes of the State Cybersecurity Act, the term “state agency” includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services. Section 282.318(2), F.S.

²⁴ “Cybersecurity” means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of data, information, and information technology resources. Section 282.0041(8), F.S.

- Adopting rules to mitigate risk, support a security governance framework, and safeguard agency digital assets, data,²⁵ information, and IT resources;²⁶
- Designating a chief information security officer (CISO);
- Developing and annually updating a statewide cybersecurity strategic plan such as identification and mitigation of risk, protections against threats, and tactical risk detection for cyber incidents;²⁷
- Developing and publishing a cybersecurity governance framework for use by state agencies;
- Assisting the state agencies in complying with the State Cybersecurity Act;
- Annually providing training on cybersecurity for managers and team members;
- Annually reviewing the strategic and operational cybersecurity plans of state agencies;
- Tracking the state agencies' implementation of remediation plans;
- Providing cybersecurity training to all state agency technology professionals that develops, assesses, and documents competencies by role and skill level;
- Maintaining a Cybersecurity Operations Center (CSOC) led by the CISO to serve as a clearinghouse for threat information and coordinate with the FDLE to support responses to incidents; and
- Leading an Emergency Support Function under the state emergency management plan.²⁸

The State Cybersecurity Act requires the head of each state agency to designate an information security manager to administer the state agency's cybersecurity program.²⁹ The head of the agency has additional tasks in protecting against cybersecurity threats as follows:

- Establish a cybersecurity incident response team with the FLDS and the Cybercrime Office, which must immediately report all confirmed or suspected incidents to the CISO;
- Annually submit to the DMS the state agency's strategic and operational cybersecurity plans;
- Conduct and update a comprehensive risk assessment to determine the security threats once every three years;
- Develop and update written internal policies and procedures for reporting cyber incidents;
- Implement safeguards and risk assessment remediation plans to address identified risks;
- Ensure internal audits and evaluations of the agency's cybersecurity program are conducted;
- Ensure that the cybersecurity requirements for the solicitation, contracts, and service-level agreement of IT and IT resources meet or exceed applicable state and federal laws, regulations, and standards for cybersecurity, including the National Institute of Standards and Technology (NIST)³⁰ cybersecurity framework;
- Provide cybersecurity training to all agency employees within 30 days of employment; and

²⁵ "Data" means a subset of structured information in a format that allows such information to be electronically retrieved and transmitted. Section 282.0041(9), F.S.

²⁶ "Information technology resources" means data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. Section 282.0041(22), F.S.

²⁷ "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur. Section 282.0041(19), F.S.

²⁸ Section 282.318(3), F.S.

²⁹ Section 282.318(4)(a), F.S.

³⁰ NIST, otherwise known as the National Institute of Standards and Technology, "is a non-regulatory government agency that develops technology, metrics, and standards to drive innovation and economic competitiveness at U.S.-based organizations in the science and technology industry." Nate Lord, *What is NIST Compliance*, DataInsider (Dec. 1, 2020), <https://www.digitalguardian.com/blog/what-nist-compliance> (last visited March 13, 2025).

- Develop a process that is consistent with the rules and guidelines established by the FLDS for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents.³¹

Florida Cybersecurity Advisory Council

The Florida Cybersecurity Advisory Council³² (CAC) within the DMS³³ assists state agencies in protecting IT resources from cyber threats and incidents.³⁴ The CAC must assist the FLDS in implementing best cybersecurity practices, taking into consideration the final recommendations of the Florida Cybersecurity Task Force – a task force created to review and assess the state’s cybersecurity infrastructure, governance, and operations.³⁵ The CAC meets at least quarterly to:

- Review existing state agency cybersecurity policies;
- Assess ongoing risks to state agency IT;
- Recommend a reporting and information sharing system to notify state agencies of new risks;
- Recommend data breach simulation exercises;
- Assist the FLDS in developing cybersecurity best practice recommendations;
- Examine inconsistencies between state and federal law regarding cybersecurity;
- Review information relating to cybersecurity and ransomware incidents [reported by state agencies and local governments] to determine commonalities and develop best practice recommendations for those entities; and
- Recommend any additional information that should be reported by a local government to FLDS as part of a cybersecurity or ransomware incident report.³⁶

The CAC must work with NIST and other federal agencies, private sector businesses, and private security experts to identify which local infrastructure sectors, not covered by federal law, are at the greatest risk of cyber-attacks and to identify categories of critical infrastructure as critical cyber infrastructure if cyber damage to the infrastructure could result in catastrophic consequences.³⁷

Each December 1, the CAC must also prepare and submit a comprehensive report to the Governor, the President of the Senate, and the Speaker of the House of Representatives that includes data, trends, analysis, findings, and recommendations for state and local action regarding ransomware incidents. At a minimum, the report must include:

- Descriptive statistics, including the amount of ransom requested, duration of the incident, and overall monetary cost to taxpayers of the incident;
- A detailed statistical analysis of the circumstances that led to the ransomware incident which does not include the name of the state agency or local government, network information, or system identifying information;

³¹ Section 282.318(4), F.S.

³² Under Florida law, an “advisory council” means an advisory body created by specific statutory enactment and appointed to function on a continuing basis. Generally, an advisory council is enacted to study the problems arising in a specified functional or program area of state government and to provide recommendations and policy alternatives. Section 20.03(7), F.S.; *See also* s. 20.052, F.S.

³³ Section 282.319(1), F.S.

³⁴ Section 282.319(2), F.S.

³⁵ Section 282.319(3), F.S.

³⁶ Section 282.319(9), F.S.

³⁷ Section 282.319(10), F.S.

- Statistical analysis of the level of cybersecurity employee training and frequency of data backup for the state agencies or local governments that reported incidents;
- Specific issues identified with current policy, procedure, rule, or statute and recommendations to address those issues; and
- Other recommendations to prevent ransomware incidents.³⁸

Cyber Incident Response

The National Cyber Incident Response Plan (NCIRP) was developed according to the direction of Presidential Policy Directive (PPD)-41,³⁹ by the U.S. Department of Homeland Security. The NCIRP is part of the broader National Preparedness System and establishes the strategic framework for a whole-of-nation approach to mitigating, responding to, and recovering from cybersecurity incidents posing risk to critical infrastructure.⁴⁰ The NCIRP was developed in coordination with federal, state, local, and private sector entities and is designed to interface with industry best practice standards for cybersecurity, including the NIST Cybersecurity Framework.

The NCIRP adopted a common schema for describing the severity of cybersecurity incidents affecting the U.S. The schema establishes a common framework to evaluate and assess cybersecurity incidents to ensure that all departments and agencies have a common view of the severity of a given incident; urgency required for responding to a given incident; seniority level necessary for coordinating response efforts; and level of investment required for response efforts.⁴¹

The severity level of a cybersecurity incident in accordance with the NCIRP is determined as follows:

- **Level 5:** An emergency-level incident within the specified jurisdiction if the incident poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local security; or the lives of the country's, state's, or local government's citizens.
- **Level 4:** A severe-level incident if the incident is likely to result in a significant impact within the affected jurisdiction which affects the public health or safety; national, state, or local security; economic security; or individual civil liberties.
- **Level 3:** A high-level incident if the incident 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.
- **Level 2:** A medium-level incident if the incident may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.
- **Level 1:** A low-level incident if the incident is unlikely to impact public health or safety; national, state, or local security; economic security; or public confidence.⁴²

³⁸ Section 282.319(12), F.S.

³⁹ Annex for PPD-41: *U.S. Cyber Incident Coordination*, available at: <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident> (last visited March 12, 2025).

⁴⁰ Cybersecurity & Infrastructure Security Agency, *Cybersecurity Incident Response*, available at <https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response#:~:text=%20National%20Cyber%20Incident%20Response%20Plan%20%28NCIRP%29%20The,incidents%20and%20how%20those%20activities%20all%20fit%20together> (last visited March 12, 2025).

⁴¹ *Id.*

⁴² Section 282.318(3)(c)9.a, F.S.

State agencies and local governments in Florida must report to the Cybersecurity Operations Center (CSOC) all ransomware incidents and any cybersecurity incidents at severity levels of 3, 4, or 5 as soon as possible, but no later than 48 hours after discovery of a cybersecurity incident and no later than 12 hours after discovery of a ransomware incident.⁴³ The CSOC is required to notify the President of the Senate and the Speaker of the House of Representatives of any incidents at severity levels of 3, 4, or 5 as soon as possible, but no later than 12 hours after receiving the incident report from the state agency or local government.⁴⁴ For state agency incidents at severity levels 1 and 2, they must report these to the CSOC and the Cybercrime Office at the FDLE as soon as possible.⁴⁵

The notification must include a high-level description of the incident and the likely effects. An incident report for a cybersecurity or ransomware incident by a state agency or local government must include, at a minimum:

- A summary of the facts surrounding the cybersecurity or ransomware incident;
- The date on which the state agency or 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;
- The types of data compromised by the cybersecurity or ransomware incident;
- The estimated fiscal impact of the cybersecurity or ransomware incident;
- In the case of a ransomware incident, the details of the ransom demanded;⁴⁶ and
- If the reporting entity is a local government, a statement requesting or declining assistance from the CSOC, FDLE Cybercrime Office, or local sheriff with jurisdiction.⁴⁷

In addition, the CSOC must provide consolidated incident reports to the President of the Senate, Speaker of the House of Representatives, and the CAC on a quarterly basis.⁴⁸ The consolidated incident reports to the CAC may not contain any state agency or local government name, network information, or system identifying information, but must contain sufficient relevant information to allow the CAC to fulfill its responsibilities.⁴⁹

State agencies and local governments are required to submit an after-action report to the FLDS within one week of the remediation of a cybersecurity or ransomware incident.⁵⁰ The report must summarize the incident, state the resolution, and any insights from the incident.

III. Effect of Proposed Changes:

Section 1 creates s. 20.70, F.S., to create the Agency for State Systems and Enterprise Technology (ASSET) to serve as Florida's centralized Information Technology (IT) governance body, overseeing statewide technology initiatives and cybersecurity efforts. The ASSET will be

⁴³ Section 282.318(3)(c)9.a, F.S.

⁴⁴ Section 282.318(3)(c)9.c.(II), F.S.

⁴⁵ Section 282.318(3)(c)9.(d), F.S.

⁴⁶ Section 282.318(3)(c)9.b, F.S.

⁴⁷ Section 282.3185(5)(a)6, F.S.

⁴⁸ Section 282.318(3)(c)9.e, F.S.

⁴⁹ *Id.*

⁵⁰ Section 282.318(4)(k), F.S, and s. 282.3185(6), F.S.

led by the Governor and Cabinet. The bill establishes the following divisions and offices within the ASSET (see Exhibit 1):

- The Division of Administrative Services; and
- The Office of Information Technology.
- Beginning July 1, 2026, the following divisions are established:
 - The Division of Enterprise Data and Interoperability.
 - The Division of Enterprise Security.
 - The Division of Enterprise Information Technology Services.
 - The Division of Enterprise Information Technology Purchasing.
 - The Division of Enterprise Information Technology Workforce Development.

The Executive Director of the ASSET serves as the State Chief Information Officer (CIO). The Governor and Cabinet must appoint a CIO from nominees of the CIO selection committee. Upon a vacancy or anticipated vacancy, the CIO selection committee within the ASSET must be appointed to nominate up to three qualified appointees for the position of CIO to the Governor and Cabinet for appointment. A member of the state CIO selection committee may designate an alternate representative if the member applies for the position.

The bill provides the selection committee must be composed of the following members:

- A state agency chief information officer of an executive agency, appointed by the Governor and who shall serve as chair of the committee.
- The chief information officer of the Department of Agriculture and Consumer Services, appointed by the Commissioner of Agriculture.
- The chief information officer of the Department of Financial Services, appointed by the Chief Financial Officer.
- The chief information officer of the Department of Legal Affairs, appointed by the Attorney General.

The appointment must be made by a majority vote of the Governor and Cabinet and is subject to confirmation by the Senate. Removal of the CIO is subject to a majority vote of the Governor and Cabinet. The CIO 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.

The bill requires the CIO to meet one of the following education requirements criteria:

- Hold a bachelor's degree from an accredited institution in IT, computer science, business administration, public administration, or a related field; or
- Hold a master's degree in any of the fields listed above, which may be substituted for a portion of the experience requirement, as determined by the selection committee.

The CIO must have at least ten years of progressively responsible experience in IT management, digital transformation, cybersecurity, or IT governance, including:

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

- Managing large-scale IT projects, enterprise infrastructure, and implementation of emerging technologies;
- Budget planning, procurement oversight, and financial management of IT investments; and
- Working with state and federal information technology regulations, digital services, and cybersecurity compliance frameworks.

As it relates to technical and policy expertise, the CIO must have demonstrated expertise in:

- Cybersecurity and data protection by demonstrating knowledge of cybersecurity risk management, compliance with National Institute for Standards and Technology (NIST), ISO 27001, and applicable federal and state security regulations;
- Cloud and digital services with experience with cloud computing, enterprise systems modernization, digital transformation, and emerging information technology trends;
- IT governance and policy development by demonstrating an understanding of statewide information technology governance structures, digital services, and information technology procurement policies; and
- Public sector information technology management by demonstrating familiarity with government information technology funding models, procurement requirements, and legislative processes affecting information technology strategy.

In addition, the bill addresses leadership and administrative experience qualifications. Specifically, the CIO must demonstrate:

- Strategic vision and innovation by possessing the capability to modernize information technology systems, drive digital transformation, and align IT initiatives with state goals;
- Collaboration and engagement with stakeholders by working with legislators, agency heads, local governments, and private sector partners to implement IT initiatives;
- Crisis management and cyber resilience by possessing the capability to develop and lead cyber incident response, disaster recovery, and IT continuity plans; and
- Fiscal management and budget expertise managing multi-million-dollar IT budgets, cost-control strategies, and financial oversight of information technology projects.

Furthermore, individuals who currently or previously served as the head of a Florida state agency are ineligible for nomination, appointment, or service as the CIO.

Section 2 provides that, until a permanent CIO is appointed, the current CIO of the Department of Management Services (DMS) must be transferred to the ASSET and serve as the interim CIO, assuming all responsibilities of the Executive Director of the ASSET. To establish long-term leadership, the Governor and Cabinet must appoint a permanent CIO by January 2, 2026. The CIO selection committee must be established by August 1, 2025, with each member of the Cabinet appointing representatives to serve on the committee.

Section 3 conforms to changes in the bill by replacing the DMS with the ASSET in s. 97.0525, F.S., relating to development of the risk assessment methodology, effective July 1, 2026.

Section 4 conforms to changes in the bill by replacing the DMS with the ASSET in s. 112.22, F.S., relating to the identification of prohibited applications, effective July 1, 2026.

Section 5 amends s. 119.0725, F.S., to make technical, conforming changes. Effective July 1, 2026, the bill implements changes related to public records exemptions. Specifically, the bill transfers cybersecurity public records exemptions and access to confidential cybersecurity data from the Florida Digital Service (FLDS) to the ASSET.

Section 6 amends s. 216.023, F.S., to continue a provision from the 2025 Implementing Bill to require that agencies provide, with their legislative budget requests, a cumulative inventory and status report for all technology-related projects with a cumulative cost of \$1 million or more. The bill defines the term “technology-related project” to mean a project that has been funded or has had or is expected to have expenditures in more than one fiscal year; has a cumulative estimated or realized cost of more than \$1 million; and does not include the continuance of existing hardware and software maintenance assessments, renewal of existing software licensing agreements, or the replacement of desktop units with the new technology that is substantially similar to the technology being replaced.

Section 7 amends s. 216.023, F.S., effective July 1, 2026, to make technical, conforming changes. It updates a cross-reference from s. 282.0051, F.S., to s. 282.0061, F.S., and repeals the provision codified in section 6 of the bill, as that information will be included within annual reporting by the ASSET.

Section 8 amends s. 282.0041, F.S., to provide the following definitions of terms:

- “Agency assessment” is repealed.
- “ASSET” means the Agency for State Systems and Enterprise Technology.
- “State agency” expands to include the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.
- “Technical Debt” means the accumulated cost and operational impact resulting from the use of suboptimal, expedient, or outdated technology solutions that require future remediation, refactoring, or replacement to ensure maintainability, security, efficiency, and compliance with enterprise architecture standards.

Section 9 removes certain powers, duties, and functions of the DMS and the FLDS. In addition, the bill modifies the responsibilities of the DMS and the FLDS in s. 282.0051, F.S., to the following:

- Begin the process of assessing and documenting existing state agency technical debt and security risks. All assessment results and documentation must be provided to the ASSET no later than June 15, 2026.
- By September 15, 2025, cybersecurity tools must be transferred from the FLDS to individual state agencies.
- The state chief information security officer will continue to receive incident reports for cybersecurity events and must submit quarterly consolidated cybersecurity incidence reports to the interim CIO, Executive Office of the Governor, the Commissioner of Agriculture, the Chief Financial Officer, the Attorney General, President of the Senate, and the Speaker of the House of Representatives.

The bill repeals s. 282.0051, F.S., relating to assigned duties and responsibilities of the DMS and the FLDS on July 1, 2026.

Section 10 repeals s. 282.00515, F.S., related to cabinet duties that are no longer applicable.

Section 11 creates s. 282.006, F.S., effective July 1, 2026, to assign duties and enterprise responsibilities to the ASSET. The bill provides the ASSET is the primary IT governance authority for the state of Florida and is responsible for setting IT policies, standards, and strategies that are adaptable and technology agnostic. In addition, the ASSET, as the lead entity, is responsible for understanding the unique state agency IT needs and environments, supporting state technology efforts, and reporting on the status of technology for the enterprise.

The bill provides that the ASSET is tasked with the following duties and responsibilities:

- Establishing the strategic direction of IT in the state.
- Developing and publishing IT policy that aligns with industry best practices for the management of the state's IT resources, which must be updated as necessary to meet requirements and advancement in technology.
- Developing, publishing, and maintaining an enterprise, in coordination with state agency technology subject matter experts, that:
 - Acknowledges the unique needs of the entities within the enterprise in the development and publication of standards and terminologies to facilitate digital interoperability;
 - Supports the cloud-first policy as specified in s. 282.206, F.S.;
 - Addresses how IT infrastructure may be modernized to achieve security, scalability, maintainability, interoperability, and improved cost-efficiency goals; and
 - Includes, at a minimum, best practices, guidelines, and standards for the following specific components:
 - Data models and taxonomies.
 - Master data management.
 - Data integration and interoperability.
 - Data security and encryption.
 - Bot prevention and data protection.
 - Data backup and recovery.
 - Application portfolio and catalog requirements.
 - Application architectural patterns and principles.
 - Technology and platform standards.
 - Secure coding practices.
 - Performance and scalability.
 - Cloud infrastructure and architecture.
 - Networking, connectivity, and security protocols.
 - Authentication, authorization, and access controls.
 - Disaster recovery.
 - Quality assurance.
 - Testing methodologies and measurements.
 - Logging and log retention.
 - Application and use of artificial intelligence.

The enterprise architecture must also include open data technical standards and enterprise testing and quality assurance best practices for functional, performance, load, security, compatibility, and interoperability testing.

The ASSET must produce the following reports and provide them to the Governor, the Commissioner of Agriculture, the Chief Financial Officer, the Attorney General, the President of the Senate, and the Speaker of the House of Representatives:

- Annually by December 15, an enterprise analysis report that includes:
 - Results of agency need assessments and plans to address any technical debt.
 - Alternative standards related to federal grant compliance.
 - IT financial data by agency for the previous fiscal year. The ASSET is required to develop a process to annually collect and report current and projected IT expenditures by each state agency, consolidating this data into a single report. Specifically, this portion of the annual report must include, at a minimum, the following recurring and nonrecurring total:
 - Number of full-time equivalent positions.
 - Amount of salary.
 - Amount of benefits.
 - Number of comparable full-time equivalent positions and total amount of expenditures for information technology staff augmentation.
 - Number of contracts and purchase orders and total amount of associated expenditures for information technology managed services.
 - Amount of expenditures by state term contract, contracts procured using alternative purchasing methods, and agency procurements through request for proposal, invitation to negotiate, invitation to bid, single source, and emergency purchases.
 - Amount of expenditures for hardware.
 - Amount of expenditures for non-cloud software.
 - Amount of expenditures for cloud software licenses and services with a separate amount for expenditures for state data center services.
 - Amount of expenditures for cloud data center services with a separate amount for expenditures for state data center services.
 - Amount of expenditures for administrative costs.
 - A consolidated IT financial analysis that outlines the anticipated funding requirements for IT support over the next five years, a current inventory of major projects, and significant unmet needs for IT resources over the next five years ranked in priority order according to their urgency.
 - Information related to the usage and key findings of the IT test laboratory established in s. 282.0065, F.S.
 - A review and summary of whether the IT contract policy is included in all solicitations and contracts.
- Biennially by December 15 of even-numbered years, a report on the strategic direction of information technology in the state that includes recommendations for the standardization of common IT services used across state agencies and for IT services that should be designed, delivered, and managed as enterprise IT services.
- A market analysis and accompanying strategic plan submitted by December 31 of each year that the market analysis is conducted. The market analysis must be conducted every three years and measure cost-effective and cost-efficient use of IT within the enterprise and the

state's adherence to best practices. The ASSET must produce a strategic plan based on the market analysis for the use and implementation of continued and future IT services.

The ASSET may adopt rules to implement the requirements in ch. 282, F.S.

Section 12 creates s. 282.0061, F.S., effective July 1, 2026, to define the ASSET's role in providing support to state agencies and oversight of state agency procurements and projects.

The Legislature intends for the ASSET to support state agencies through the adoption of policies, standards, and guidance and by providing oversight that recognizes unique state agency information technology needs, environments, and goals. The ASSET assistance and support must allow for adaptability to emerging technologies and organizational needs while maintaining compliance with industry best practices. The ASSET is prohibited from prescribing specific tools, platforms, or vendors.

The bill requires that the baseline needs assessments for state agencies be completed by January 1, 2028, and use the Capability Maturity Model⁵¹ for measuring each agency's IT capabilities in for each domain. Once completed, the assessments must be maintained and updated on a regular schedule adopted by the ASSET. The ASSET must submit a plan and schedule to complete the baseline needs assessments to the Governor, the Commissioner of Agriculture, the Chief Financial Officer, the Attorney General, the President of the Senate, and the Speaker of the House of Representatives by October 1, 2026. The needs assessments must include documentation of each agency's:

- Distinct technical environments;
- Existing technical debt;
- Security risks; and
- Compliance with all information technology standards and guidelines developed and published by the ASSET.

In assessing the existing technical debt portion of the needs assessment, the ASSET must 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;
- Required capabilities not available with the legacy system;
- The estimated process, timeline, and cost to migrate from legacy environments;
- The estimated time frame during which the state agency can continue to efficiently use legacy information technology system, resources, security, and data management to support operations; and
- Any other information necessary for fiscal or technology planning.

⁵¹ The Capability Maturity Model (CMM) ranks software development enterprises according to a hierarchy of five process maturity levels. Each level ranks the development environment according to its capability of producing quality software. A set of standards is associated with each of the five levels. The standards for level one describe the most immature or chaotic processes, and the standards for level five describe the most mature or quality processes. This maturity model indicates the degree of reliability or dependency a business can place on a process to achieve its desired goals or objectives. It is also a collection of instructions that an enterprise can follow to gain better control over its software development process.

State agencies are required to provide all necessary documentation to enable accurate reporting on legacy systems and, with support from the ASSET, produce a phased roadmap to address known technology gaps, deficiencies, and advancement of the agency's maturity level in accordance with the Capability Maturity Model. The roadmaps must be maintained and submitted annually with the state agencies' legislative budget requests.

The bill requires that the following be considered and included in the ASSET's annual report:

- Potential methods for standardizing data across state agencies which will promote interoperability and reduce the collection of duplicative data.
- Opportunities for standardization and consolidation of information technology services that are common across all state agencies and that support improved:
 - Interoperability;
 - Security;
 - Scalability;
 - Maintainability;
 - Cost efficiency;
 - Business functions; and
 - Operations.

Additionally, the ASSET must develop statewide standards for master data management (MDM) to enable data sharing and interoperability, with a strategy for implementing enterprise MDM to be submitted to the Governor, the Commissioner of Agriculture, the Chief Financial Officer, the Attorney General, the President of the Senate, and the Speaker of the House of Representatives by December 1, 2028. The report must include the vision, goals, and benefits of implementing a statewide master data management initiative, an analysis of the current state, and the recommended strategy, methodology, and estimated timeline and resources needed at a state agency and enterprise level to accomplish the initiative.

The ASSET will support state agency IT projects by:

- Providing procurement advisory and review services for information technology projects to all state agencies, including procurement and contract development assistance.
- Establishing best practices and enterprise procurement processes and metrics.
- Upon request, assisting agencies with the development of IT related legislative budget requests.
- Developing IT project standards and oversight measures that objectively provide data regarding the project status, require mandatory reporting when an IT project is one month late or exceeds its budget by \$1 million, and require compliance with the enterprise architecture.
- Developing standardized information technology project reporting templates for use by state agencies.
- Providing project management and oversight training opportunities to state agencies.
- Performing project oversight on projects with a total project cost of \$10 million or more and reporting quarterly on any IT project that ASSET identifies as high-risk.
- Establishing a streamlined reporting process with clear timelines and procedures to notify a state agency if there is deviation from the adopted standards.

The bill also charges the ASSET to consult with state agencies to create a methodology, approach, and applicable templates and formats for identifying and collecting both current and planned information technology expenditure data at the state agency level. State agencies must provide financial data to the ASSET annually by October 1 for the previous fiscal year.

State agencies must work with the ASSET to establish alternative standards and policies if adherence to standards or policies published by the ASSET conflict with federal regulations or requirements and results in, or is expected to result in, adverse action against the state agencies or loss of federal funding.

Section 13 creates s. 282.0062, F.S., effective July 1, 2026, to establish multiple enterprise-level IT workgroups within the ASSET to foster collaboration among state agencies and standardize IT policies, governance, security, and procurement. Each workgroup will consist of representatives from all state agencies and provide recommendations to the ASSET leadership on key areas such as cybersecurity, data interoperability, IT operations, quality assurance, project management, contract oversight, and procurement. Additionally, state IT leaders, including the CIO, Chief Information Security Officer, Chief Data Officer, Chief Technology Officer, Chief Information Technology Procurement Officer, and others will consult with these workgroups on a quarterly basis to ensure continuous improvement in IT governance and strategy (see Exhibit 1).

Section 14 creates s. 282.0063, F.S., effective July 1, 2026, to address the ASSET's role in IT workforce development. The ASSET is required to consult with CareerSource Florida, Inc., the Department of Commerce, and the Department of Education to carry out the tasks in this section. The ASSET will develop structured career paths, training programs, and workforce strategies to enhance the recruitment, retention, and skill development of state IT professionals. This includes conducting a comprehensive workforce needs assessment to identify and address IT skill gaps, improving agency capabilities. The ASSET will also create a statewide training program to help agencies implement enterprise architecture policies and standards. Additionally, the ASSET is responsible for developing new training programs and certifications to ensure state IT professionals stay current with cybersecurity, cloud computing, and emerging technologies. To strengthen the state's IT talent pipeline, the ASSET will establish internship and scholarship-for-service programs. Furthermore, in coordination with the Department of Management Services, ASSET will create standardized IT career progression frameworks and leadership development initiatives to support employee retention and professional growth.

Section 15 creates 282.0064, F.S., effective July 1, 2026, to define the ASSET's responsibilities related to IT contracts and procurements. The ASSET will oversee all IT procurement policies to ensure consistency, compliance, and cost-effectiveness across state agencies. All IT contracts must align with enterprise architecture standards and adhere to National Institute of Standards and Technology Cybersecurity Framework (NIST) cybersecurity requirements.

For projects exceeding \$10 million, independent verification and validation (IV&V) will be required. The IV&V provider must provide a report directly to stakeholders that includes an analysis of whether:

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

- The project is adhering to established project management processes.
- The procurement of products, tools, and services and resulting contracts align with current statutory and regulatory requirements.
- The value of services delivered is commensurate with project costs.
- The completed project meets the actual needs of the intended users.

Additionally, the ASSET will coordinate with the DMS to evaluate responses and answer vendor questions for IT related state term contracts.

Section 16 creates s. 282.0065, F.S., effective July 1, 2026, to instruct the ASSET to establish an IT Test Laboratory beginning July 1, 2027, or after all elements of the enterprise architecture are published, whichever is later, and subject to appropriation.

The IT Test Laboratory will provide state agencies with a controlled environment to evaluate technology before procurement, allowing agencies to refine their procurement requirements based on real-world testing to avoid costly IT failures. The ASSET will oversee the lab's operations, security, compliance, and access to emerging technologies in collaboration with industry partners. The ASSET may also leverage public-private partnerships to enhance lab operations while ensuring state agencies have access to the latest technological advancements. Furthermore, the ASSET will develop standardized policies, procedures, and eligibility criteria to govern agency access and use of the test laboratory.

Section 17 creates s. 282.066, F.S., to task the ASSET with developing, implementing, and maintaining a library to serve as the official repository for all enterprise IT policies, standards, guidelines, and best practices applicable to state agencies. This online library will be accessible to all state agencies through a secure authentication system, featuring a structured index and search functionality to facilitate the efficient retrieval of information.

The library will be regularly updated to reflect current state and federal requirements, industry best practices, and emerging technologies. It will include standardized checklists organized by technical subject areas to assist agencies in measuring compliance with IT policies, standards, and best practices.

The ASSET is required to establish procedures to ensure the integrity, security, and availability of the library, including access controls, encryption, and disaster recovery measures. The ASSET will maintain version control and revision history for all published documents and provide mechanisms for agencies to submit feedback, request clarifications, and recommend updates. All state agencies are required to reference and adhere to the policies, standards, guidelines, and best practices contained in the library when planning, procuring, implementing, and operating IT systems.

The bill also provides a compliance exception process. Agencies may request an exception to a specific policy, standard, or guideline if compliance is not technically feasible, would cause undue hardship, or conflicts with agency-specific statutory requirements. The requesting agency must submit a formal justification detailing the specific requirement, reasons for non-compliance, any compensating controls, and the expected duration of the exception. The ASSET will review all exception requests and provide a recommendation to the state chief information

officer, who will then present the requests to the chief information officer workgroup for approval by a majority vote. Approved exceptions will be documented, with conditions or expiration dates noted. Agencies granted exceptions will undergo periodic reviews to determine if the exception remains necessary or if compliance can now be achieved.

Section 18 amends s. 282.318, F.S., effective July 1, 2025, to remove the following responsibilities from the Florida Digital Service (FLDS):

- Development and updating of a statewide cybersecurity strategic plan.
- Development and publication of guidelines related to:
 - Establishing asset management procedures;
 - Using standard risk assessment methodology;
 - Completing comprehensive risk assessments and cybersecurity audits;
 - Identifying protection procedures to manage protection of state assets;
 - Establishing procedures for securely accessing information;
 - Detecting threats through proactive monitoring;
 - Establishing procedures for procuring IT commodities and services; and
 - Recovering information and data in response to a cybersecurity incident.
- Operation and maintenance of a Cybersecurity Operations Center.
- Leading an Emergency Support Function, ESF CYBER, under the state comprehensive emergency management plan.

The bill also provides for incident reporting to and through the state chief information security officer in place of the cybersecurity operations center; changes the timeline for reporting incidents with severity levels 3, 4, or 5 from 48 hours to 12 hours; and, for reporting incidents with severity levels of 1 or 2, requires reporting within 96 hours of a cybersecurity incident and 72 hours of a ransomware incident.

Additionally, the bill changes the timeframe for state agencies to provide state agency strategic cybersecurity plans and conduct comprehensive risk assessments from once every three years to once every two years. The state agency cybersecurity plans must include measures that assess performance against their risk management plan. The biennial cybersecurity risk assessments must include vulnerability and penetration testing and acknowledge that agency leadership is aware of the risks outlined in the report.

Section 19 amends s. 282.318, F.S., effective July 1, 2026, by updating the reference to cabinet agencies in the definition of a state agency, naming the ASSET as the lead entity responsible for establishing enterprise technology and cybersecurity standards, and replacing remaining references to the Florida Digital Service. This section also adds the following responsibilities to the ASSET, which are the same as those currently required for the FLDS:

- Development and updating of a statewide cybersecurity strategic plan.
- Development and publication of guidelines related to:
 - Establishing asset management procedures;
 - Using standard risk assessment methodology;
 - Completing comprehensive risk assessments and cybersecurity audits;
 - Identifying protection procedures to manage protection of state assets;
 - Establishing procedures for securely accessing information;
 - Detecting threats through proactive monitoring;

- Establishing procedures for procuring IT commodities and services; and
- Recovering information and data in response to a cybersecurity incident.

Section 20 amends s. 282.3185, F.S., effective July 1, 2025, related to local government cybersecurity to make conforming changes made in the bill. The state chief information security officer will now receive incident reports in place of the FLDS and the cybersecurity operations center. The bill also deletes references to the Cybersecurity Advisory Council.

Section 21 amends, and makes technical, conforming changes to s. 282.3185, F.S., effective July 1, 2026, related to local government cybersecurity. The ASSET will maintain the current cybersecurity severity levels and incident reporting processes for local governments, ensuring continuity in managing security incidents. Specifically, the bill the timeline for reporting incidents with severity levels 3, 4, or 5 changes from 48 hours to 12 hours after discovery of the cybersecurity incident and no later than 6 hours (instead of 12) after discovery of a ransomware incident. The bill also updates relevant statutory references.

Section 22 repeals s. 282.319, F.S., effective July 1, 2025, related to the Cybersecurity Advisory Council. These activities will generally be within the scope of the ASSET duties and responsibilities.

Section 23 outlines a plan for fully staffing the ASSET with the necessary specialized personnel to oversee IT governance, procurement, and security for all Florida state agencies. It provides the ASSET with a structured leadership team, including key positions such as the state chief information officer, state chief technology officer, state chief information security officer, state chief data officer, state chief IT procurement officer, and state chief of IT workforce development. Additionally, the ASSET technology subject matter experts will be assigned across major state agency program areas to support the understanding of each agency's technical and operational environments. To further enhance its operations, the ASSET will include bureaus dedicated to specific program areas, including IT needs analysis, quality assurance, project management, contract management, and procurement (see Exhibit 1).

Specifically, the bill establishes the following positions within the ASSET:

- Chief operations officer.
- Chief information officer.
- Effective July 1, 2026, the following must be appointed by the CIO of the ASSET:
 - Deputy executive director, who shall serve as the state chief information architect.
 - A minimum of six lead technology coordinators. At least one coordinator must be assigned to each of the following major program areas: health and human services, education, government operations, criminal and civil justice, agriculture and natural resources, and transportation and economic development.
 - A minimum of six assistant technology coordinators. At least one coordinator must be assigned to each of the following major program areas: health and human services, education, government operations, criminal and civil justice, agriculture and natural resources, and transportation and economic development.
 - State chief information security officer and six lead security consultants. One consultant must be assigned to each of the following major program areas: health and

- human services, education, government operations, criminal and civil justice, agriculture and natural resources, and transportation and economic development.
- State chief data officer.
 - A minimum of three data specialists with at least one specialist dedicated to each of the areas of expertise including, personally identifiable information, protected health information, and criminal justice information services.
 - A minimum of six data security consultants. At least one consultant must be assigned to each of the following major program areas: health and human services, education, government operations, criminal and civil justice, agriculture and natural resources, and transportation and economic development.
 - State chief information technology procurement officer.
 - A minimum of six lead information technology procurement consultants. At least one coordinator must be assigned to each of the following major program areas: health and human services, education, government operations, criminal and civil justice, agriculture and natural resources, and transportation and economic development.
 - State chief technology officer.
 - A minimum of 42 information technology business analyst consultants that must be assigned to major program areas as follows:
 - At least 11 consultants shall be assigned to health and human services and dedicated to state agencies.
 - At least four consultants shall be assigned to education.
 - At least eight consultants shall be assigned to government operations and dedicated to state agencies.
 - At least six consultants shall be assigned to criminal and civil justice and dedicated to state agencies.
 - At least four consultants shall be assigned to agriculture and natural resources and dedicated to state agencies.
 - At least nine consultants shall be assigned to transportation and economic development and dedicated to state agencies
 - A minimum of six information technology project management professional consultants. At least one consultant must be assigned to each of the following major program areas: health and human services, education, government operations, criminal and civil justice, agriculture and natural resources, and transportation and economic development.
 - A minimum of six information technology contract management consultants. At least one consultant must be assigned to each of the following major program areas: health and human services, education, government operations, criminal and civil justice, agriculture and natural resources, and transportation and economic development.
 - A minimum of six information technology quality assurance consultants. At least one consultant must be assigned to each of the following major program areas: health and human services, education, government operations, criminal and civil justice, agriculture and natural resources, and transportation and economic development.
 - State chief of information technology workforce development.

This bill also creates a state agency CIO policy workgroup, chaired by the interim state chief information officer, to provide legislative recommendations by December 1, 2025, on the structure, budget, and governance of ASSET before it becomes fully operational. The full

workgroup consists of all interested state agency chief information officers. The voting members of the workgroup include the chair of the workgroup and the chief information officers from the Department of Financial Services, the Department of Agriculture and Consumer Services, and the Department of Legal Affairs. The final report must be voted on and accepted by a unanimous vote of the voting members of the workgroup. The workgroup will dissolve after submitting its final report.

Section 24 deletes obsolete language in s. 282.201, F.S., related to the DMS management of the state data center, requires the Northwest Regional Data Center (NWRDC) to meet or exceed the state's technology standards, and permanently codifies an exception for data center use for the Division of Emergency Management done in the implementing bill in Fiscal Year 2024-2025.

Section 25 creates s. 282.0211, F.S., regarding the state data center services provided by the NWRDC to put the data center into the appropriate chapter of law. It also makes technical, conforming changes to update relevant statutory references and includes a requirement that the NWRDC provide projected costs for state data center services to the Executive Office of the Governor and the Legislature by November 15 of each year.

Section 26 amends s. 1004.649, F.S., by deleting the provisions regarding the state data center services provided by the NWRDC that were added to s. 282.0211, F.S. It also creates the NWRDC at the Florida State University and specifies the NWRDC is the designated state data center with a reference to the state data center duties outlined in s. 282.0211, F.S.

Section 27 abolishes the FLDS within the DMS in s. 20.22, F.S., effective July 1, 2026.

Section 28 amends s. 282.802, F.S., effective July 1, 2026, to transfer the Government Technology Modernization Council from the DMS to the ASSET, names the CIO as the nonvoting executive director of the council, and makes other conforming changes.

Section 29 amends s. 282.604, F.S., effective July 1, 2026, by transitioning rulemaking authority regarding accessible electronic information technology by governmental units from the Department of Management Services to the ASSET.

Section 30 requires the CIO, instead of the FLDS, to participate in the process for technology state term contract solicitations in s. 287.0591, F.S.

Section 31 makes technical, conforming changes to cross-references in s. 288.012, F.S.

Section 32 requires the Department of Commerce to consult with the ASSET in place of the FLDS regarding the Reemployment Assistance Claims and Benefits Information System in s. 443.1113, F.S., effective July 1, 2026.

Section 33 requires the FDLE to consult with the state chief information security officer in place of the FLDS when adopting rules related to IT security provisions in s. 943.0415, F.S., effective July 1, 2026.

Section 34 deletes the requirement that a request for assistance with a cybersecurity incident must come from the FLDS in s. 1004.444, F.S., effective July 1, 2026.

Section 35 provides that, except as otherwise expressly provided, the bill takes effect July 1, 2025.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The bill has a significant negative fiscal impact on state expenditures. The fiscal impact for Fiscal Year 2025-2026 for the newly created Agency for State Systems and Enterprise Technology (ASSET) is \$3,473,058 and 22 positions, which can be absorbed within existing resources via transfer from the Florida Digital Service (FDS) within the General Appropriations Act. For Fiscal Year 2026-2027, the estimated need for the newly created ASSET is a total of 197 positions and a recurring \$30,097,022 and nonrecurring \$11,297,836. This will be offset by \$11,445,979 in recurring funds from the elimination of the FDS for a net estimated recurring impact of 127 positions and \$18,651,043.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 20.22, 97.0525, 122.22, 119.0725, 216.023, 282.0041, 282.0051, 282.201, 282.318, 282.3185, 282.802, 282.604, 287.0591, 288.012, 443.1113, 943.0415, 1004.444, and 1004.649.

This bill creates the following sections of the Florida Statutes: 20.70, 282.006, 282.0061, 282.0062, 282.0063, 282.0064, 282.0065, 282.0066, and 282.0211.

This bill repeals the following sections of the Florida Statutes: 282.00515 and 282.319.

IX. Additional Information:**A. Committee Substitute – Statement of Changes:**

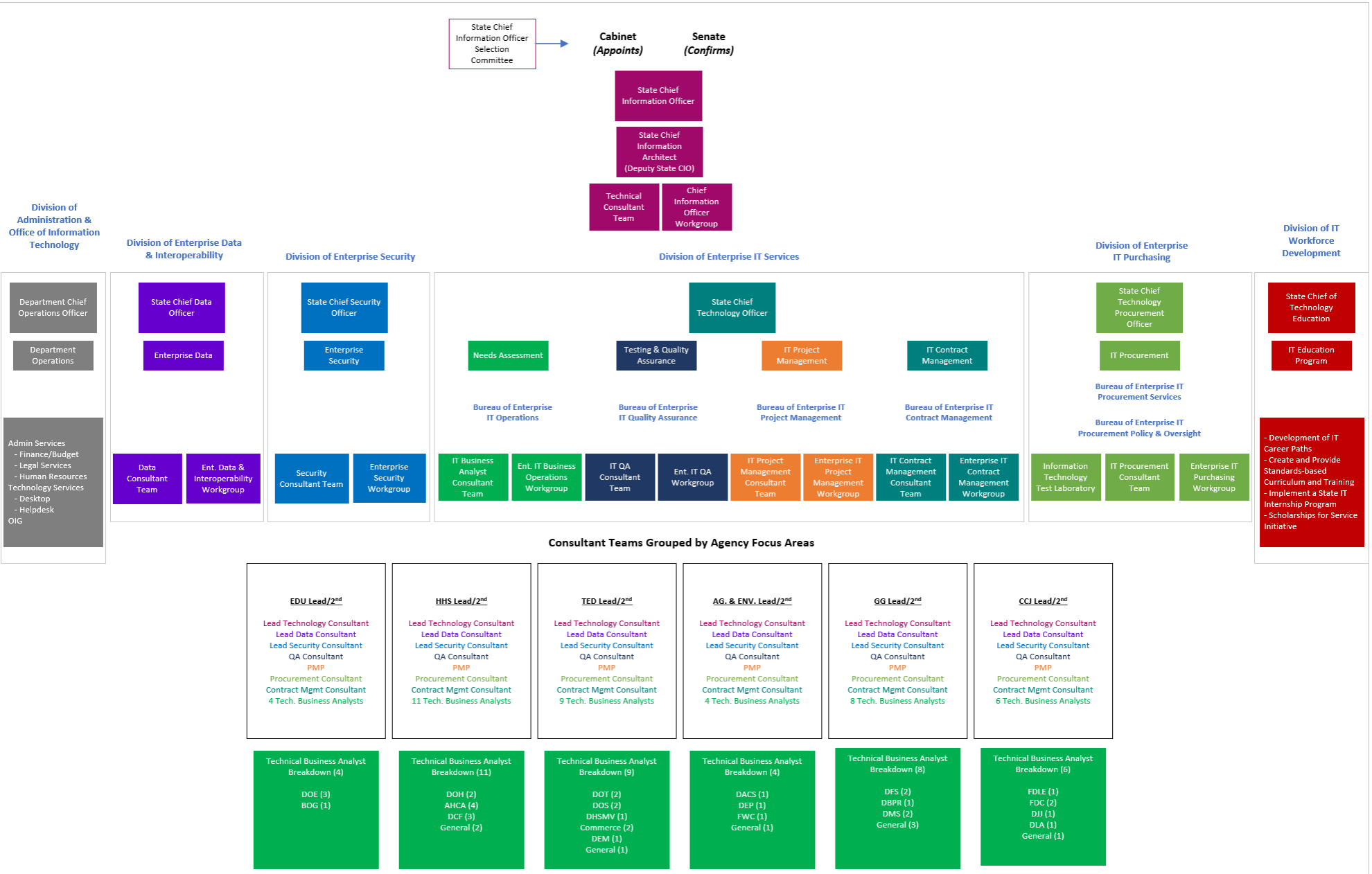
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.

Exhibit 1





464614

LEGISLATIVE ACTION

Senate	.	House
Comm: FAV	.	
03/20/2025	.	
	.	
	.	
	.	

The Committee on Appropriations (Harrell) recommended the following:

Senate Amendment (with title amendment)

Between lines 375 and 376

insert:

(c) If a member of the selection committee submits an application to be considered for the position of state chief information officer, the member must designate an alternate state agency chief information officer to serve on the committee.



464614

11 ===== T I T L E A M E N D M E N T =====

12 And the title is amended as follows:

13 Delete line 18

14 and insert:

15 providing the composition of such committee; requiring
16 that a member of the committee designate an alternate
17 state agency chief information officer to serve on the
18 committee under a specified circumstance; providing



208734

LEGISLATIVE ACTION

Senate	.	House
Comm: FAV	.	
03/20/2025	.	
	.	
	.	
	.	

The Committee on Appropriations (Harrell) recommended the following:

- 1 **Senate Amendment**
- 2
- 3 Delete line 710
- 4 and insert:
- 5 Administrative Commission;



784910

LEGISLATIVE ACTION

Senate	.	House
Comm: FAV	.	
03/20/2025	.	
	.	
	.	
	.	

The Committee on Appropriations (Harrell) recommended the following:

Senate Amendment

Delete lines 1324 - 1459
and insert:

(h) 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 ASSET.

(6) INFORMATION TECHNOLOGY FINANCIAL DATA.—

(a) In consultation with state agencies, ASSET shall create



784910

11 a methodology, an approach, and applicable templates and formats
12 for identifying and collecting both current and planned
13 information technology expenditure data at the state agency
14 level. ASSET shall continuously obtain, review, and maintain
15 records of the appropriations, expenditures, and revenues for
16 information technology for each state agency.

17 (b) ASSET shall prescribe the format for state agencies to
18 provide all necessary financial information to ASSET for
19 inclusion in the annual report required under s. 282.006. State
20 agencies must provide the information to ASSET by October 1 for
21 the previous fiscal year. The information must be reported by
22 ASSET in order to determine all costs and expenditures for
23 information technology assets and resources provided by the
24 state agencies or through contracts or grants.

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

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

35 282.0062 ASSET workgroups.—The following workgroups are
36 established within ASSET to facilitate coordination with state
37 agencies:

38 (1) CHIEF INFORMATION OFFICER WORKGROUP.—

39 (a) The chief information officer workgroup, composed of



784910

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

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

54 (2) ENTERPRISE DATA AND INTEROPERABILITY WORKGROUP.—

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

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

66 (3) ENTERPRISE SECURITY WORKGROUP.—

67 (a) The enterprise security workgroup, composed of chief
68 information security officer representatives from all state



784910

69 agencies, shall consider and make recommendations to the state
70 chief information security officer on such matters as
71 cybersecurity policies, standards, services, and architecture
72 that promote the protection of state assets.

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

78 (4) ENTERPRISE INFORMATION TECHNOLOGY OPERATIONS
79 WORKGROUP.—

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

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

92 (5) ENTERPRISE INFORMATION TECHNOLOGY QUALITY ASSURANCE
93 WORKGROUP.—

94 (a) The enterprise information technology quality assurance
95 workgroup, composed of testing and quality assurance
96 representatives from all state agencies, shall consider and make
97 recommendations to the state chief technology officer on such



784910

98 matters as testing methodologies, tools, and best practices to
99 reduce risks related to software defects, cybersecurity threats,
100 and operational failures.

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

106 (6) ENTERPRISE INFORMATION TECHNOLOGY PROJECT MANAGEMENT
107 WORKGROUP.—

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

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

120 (7) ENTERPRISE INFORMATION TECHNOLOGY CONTRACT MANAGEMENT
121 WORKGROUP.—

122 (a) The enterprise information technology contract
123 management workgroup, composed of information technology
124 contract manager representatives from all state agencies, shall
125 consider and make recommendations to the state chief technology
126 officer on such matters as information technology contract



784910

127 management policies and standards that promote best practices
128 for vendor oversight, risk management and compliance, and
129 performance monitoring and reporting across the enterprise.

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

134 (8) ENTERPRISE INFORMATION TECHNOLOGY PURCHASING
135 WORKGROUP.—

136 (a) The enterprise information technology purchasing
137 workgroup, composed of information technology procurement
138 representatives from all state agencies, shall consider and make
139 recommendations to the state chief information technology
140 procurement officer on such matters as information technology
141 procurement policies, standards, and purchasing strategy and
142 optimization that promote best practices for contract
143 negotiation, consolidation, and effective service-level
144 agreement implementation across the enterprise.

145 (b) At a minimum, the state chief information technology
146 procurement



867736

LEGISLATIVE ACTION

Senate	.	House
Comm: FAV	.	
03/20/2025	.	
	.	
	.	
	.	

The Committee on Appropriations (Harrell) recommended the following:

Senate Amendment (with title amendment)

Delete lines 2537 - 2901

and insert:

6. State chief of information technology workforce development.

(2) BUREAUS.-

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

1. The Bureau of Enterprise Information Technology



867736

11 Operations, responsible for assessing state agency information
12 technology needs and risks as established under s. 282.006,
13 Florida Statutes.

14 2. The Bureau of Enterprise Information Technology Quality
15 Assurance, responsible for activities established under s.
16 282.006, Florida Statutes.

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

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

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

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

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

31 (3) WORKGROUP.—

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

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

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



867736

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

45 (e) The chair of the workgroup shall submit a report to the
46 Governor, the Commissioner of Agriculture, the Chief Financial
47 Officer, the Attorney General, the President of the Senate, and
48 the Speaker of the House of Representatives which includes
49 recommendations and justifications for changes by December 1,
50 2025. The final report must be voted on and accepted by a
51 unanimous vote of the voting members of the workgroup.

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

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

56 282.201 State data center.—The state data center is
57 established within the Northwest Regional Data Center pursuant
58 to s. 282.0211 and shall meet or exceed the information
59 technology standards specified in ss. 282.006 and 282.318 ~~the~~
60 ~~department. The provision of data center services must comply~~
61 ~~with applicable state and federal laws, regulations, and~~
62 ~~policies, including all applicable security, privacy, and~~
63 ~~auditing requirements. The department shall appoint a director~~
64 ~~of the state data center who has experience in leading data~~
65 ~~center facilities and has expertise in cloud computing~~
66 ~~management.~~

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

68 ~~(a) Offer, develop, and support the services and~~



867736

69 ~~applications defined in service-level agreements executed with~~
70 ~~its customer entities.~~

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

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

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

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

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

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

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

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

97 ~~6. Provide a timely billing methodology to recover the~~



867736

98 ~~costs of services provided to the customer entity pursuant to s.~~
99 ~~215.422.~~

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

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

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

111 ~~10. Provide for mediation of disputes by the Division of~~
112 ~~Administrative Hearings pursuant to s. 120.573.~~

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

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

119 ~~1. Upon consolidation, a state agency shall relinquish~~
120 ~~administrative rights to consolidated resources and equipment.~~
121 ~~State agencies required to comply with federal and state~~
122 ~~criminal justice information security rules and policies shall~~
123 ~~retain administrative access rights sufficient to comply with~~
124 ~~the management control provisions of those rules and policies;~~
125 ~~however, the state data center shall have the appropriate type~~
126 ~~or level of rights to allow the center to comply with its duties~~



867736

127 ~~pursuant to this section. The Department of Law Enforcement~~
128 ~~shall serve as the arbiter of disputes pertaining to the~~
129 ~~appropriate type and level of administrative access rights~~
130 ~~pertaining to the provision of management control in accordance~~
131 ~~with the federal criminal justice information guidelines.~~

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

137 ~~(g) In its procurement process, show preference for cloud-~~
138 ~~computing solutions that minimize or do not require the~~
139 ~~purchasing, financing, or leasing of state data center~~
140 ~~infrastructure, and that meet the needs of customer agencies,~~
141 ~~that reduce costs, and that meet or exceed the applicable state~~
142 ~~and federal laws, regulations, and standards for cybersecurity.~~

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

148 ~~(1)(2) USE OF THE STATE DATA CENTER.—~~

149 ~~(a) The following are exempt from the use of the state data~~
150 ~~center: the Department of Law Enforcement, the Department of the~~
151 ~~Lottery's Gaming System, Systems Design and Development in the~~
152 ~~Office of Policy and Budget, the regional traffic management~~
153 ~~centers as described in s. 335.14(2) and the Office of Toll~~
154 ~~Operations of the Department of Transportation, the State Board~~
155 ~~of Administration, state attorneys, public defenders, criminal~~



867736

156 conflict and civil regional counsel, capital collateral regional
157 counsel, ~~and~~ the Florida Housing Finance Corporation, and the
158 Division of Emergency Management within the Executive Office of
159 the Governor.

160 ~~(b) The Division of Emergency Management is exempt from the~~
161 ~~use of the state data center. This paragraph expires July 1,~~
162 ~~2025.~~

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

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

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

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

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

179 ~~(b) Developing and implementing cost-recovery mechanisms~~
180 ~~that recover the full direct and indirect cost of services~~
181 ~~through charges to applicable customer entities. Such cost-~~
182 ~~recovery mechanisms must comply with applicable state and~~
183 ~~federal regulations concerning distribution and use of funds and~~
184 ~~must ensure that, for any fiscal year, no service or customer~~



867736

185 ~~entity subsidizes another service or customer entity. The~~
186 ~~department may recommend other payment mechanisms to the~~
187 ~~Executive Office of the Governor, the President of the Senate,~~
188 ~~and the Speaker of the House of Representatives. Such mechanisms~~
189 ~~may be implemented only if specifically authorized by the~~
190 ~~Legislature.~~

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

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

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

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

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



867736

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

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

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

227 ~~(d) In collaboration with the Department of Law Enforcement~~
228 ~~and the Florida Digital Service, developing and implementing a~~
229 ~~process for detecting, reporting, and responding to~~
230 ~~cybersecurity incidents, breaches, and threats.~~

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

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



867736

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

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

253 Section 25. Section 282.0211, Florida Statutes, is created
254 to read:

255 282.0211 Northwest Regional Data Center.—

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

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

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

270 (c) Enter into a service-level agreement with each state
271 agency customer to provide services as defined and approved by



867736

272 the governing board of the center. At a minimum, such service-
273 level agreements must:

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

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

280 3. Identify the scope of work;

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

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

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

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

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

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

300 10. Provide state agency customer entities with access to



867736

301 applications, servers, network components, and other devices
302 necessary for entities to perform business activities and
303 functions and as defined and documented in a service-level
304 agreement.

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

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

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

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

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

328 (i) Provide a plan for consideration by the Legislative
329 Budget Commission if the governing body of the center approves



867736

330 the use of a billing rate schedule after the start of the fiscal
331 year that increases any state agency customer's costs for that
332 fiscal year.

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

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

341 (l) Submit invoices to state agency customers.

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

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

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

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

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

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



867736

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

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

364 (4) If such authority is terminated, the center has 1 year
365 to provide for the transition of its state agency customers to a
366 qualified alternative cloud-based data center that meets the
367 enterprise architecture standards established pursuant to this
368 chapter.

369 Section 26. Section 1004.649, Florida Statutes, is amended
370 to read:

371 1004.649 Northwest Regional Data Center.—There is created
372 at Florida State University the Northwest Regional Data Center.
373 The data center shall serve as the state data center as
374 designated in s. 282.201

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

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

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



867736

388 ~~distribution and use of state and federal funds.~~

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

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

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

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

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

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

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

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

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

414 ~~9. Provide that the service-level agreement may be~~
415 ~~terminated by either party for cause only after giving the other~~
416 ~~party notice in writing of the cause for termination and an~~



867736

417 ~~opportunity for the other party to resolve the identified cause~~
418 ~~within a reasonable period; and~~

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

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

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

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

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

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



867736

446 ~~fiscal year.~~

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

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

455 ~~(k) Prepare and submit state agency customer invoices to~~
456 ~~the Department of Management Services for approval. Upon~~
457 ~~approval or by default pursuant to s. 282.201(5), submit~~
458 ~~invoices to state agency customers.~~

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

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

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

467 ~~(b) Procure third party cloud computing services without~~
468 ~~evaluating the cloud computing services provided by the~~
469 ~~Northwest Regional Data Center.~~

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

473 ~~(3) The Northwest Regional Data Center's authority to~~
474 ~~provide data center services to its state agency customers may~~



867736

475 ~~be terminated if:~~

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

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

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

486

487 ===== T I T L E A M E N D M E N T =====

488 And the title is amended as follows:

489 Delete lines 275 - 292

490 and insert:

491 duties; amending s. 282.201, F.S.; establishing the
492 state data center within the Northwest Regional Data
493 Center; requiring the Northwest Regional Data Center
494 to meet or exceed specified information technology
495 standards; revising requirements of the state data
496 center; abrogating the scheduled repeal of the
497 Division of Emergency Management's exemption from
498 using the state data center; deleting Department of
499 Management Services' responsibilities related to the
500 state data center; deleting provisions relating to
501 contracting with the Northwest Regional Data Center;
502 creating s. 282.0211, F.S.; designating the Northwest
503 Regional Data Center as a state data center for all



867736

504 state agencies; requiring the data center to engage in
505 specified actions; prohibiting state agencies from
506 terminating services with the data center without
507 giving written notice within a specified timeframe,
508 procuring third-party cloud-computing services without
509 evaluating the data center's cloud-computing services,
510 and exceeding a specified timeframe to remit payments
511 for data center services provided by the data center;
512 specifying circumstances under which the data center's
513 designation may be terminated; providing that the data
514 center has a specified timeframe to provide for the
515 transition of state agency customers to a qualified
516 alternative cloud-based data center that meets
517 specified standards; amending s. 1004.649, F.S.;
518 creating the Northwest Regional Data Center at Florida
519 State University; conforming provisions to changes
520 made by the act;

FOR CONSIDERATION By the Committee on Appropriations

576-02447-25

20257026pb

1 A bill to be entitled
 2 An act relating to information technology; creating s.
 3 20.70, F.S.; creating the Agency for State Systems and
 4 Enterprise Technology (ASSET); providing that the
 5 Governor and Cabinet are the head of the agency;
 6 establishing divisions and offices of the agency;
 7 providing for an executive director of the agency;
 8 providing that the executive director also serves as
 9 the state chief information officer; providing for the
 10 appointment and removal of such executive director;
 11 prohibiting the state chief information officer from
 12 having financial, personal, or business conflicts of
 13 interest related to certain vendors, contractors, and
 14 service providers of the state; requiring that the
 15 state chief information officer selection committee
 16 within ASSET be appointed and provide a specified
 17 number of nominees upon a vacancy of such officer;
 18 providing the composition of such committee; providing
 19 the qualifications for the state chief information
 20 officer; providing that persons who currently serve,
 21 or have served, as state agency heads are ineligible
 22 to serve as the state chief information officer;
 23 transferring the state chief information officer of
 24 the Department of Management Services to ASSET until
 25 the Governor and the Cabinet appoint a permanent
 26 officer; requiring that such appointment occur by a
 27 specified date; amending s. 97.0525, F.S.; requiring
 28 that the Division of Elections comprehensive risk
 29 assessment comply with the risk assessment methodology

Page 1 of 107

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

576-02447-25

20257026pb

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

Page 2 of 107

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

576-02447-25

20257026pb

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

Page 3 of 107

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

576-02447-25

20257026pb

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

Page 4 of 107

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

576-02447-25

20257026pb

117 report; providing the duties and responsibilities of
 118 ASSET related to state agency technology projects;
 119 requiring ASSET, in consultation with state agencies,
 120 to create a methodology, approach, and applicable
 121 templates and formats for identifying and collecting
 122 information technology expenditure data at the state
 123 agency level; requiring ASSET to obtain, review, and
 124 maintain records of the appropriations, expenditures,
 125 and revenues for information technology for each state
 126 agency; requiring ASSET to prescribe the format for
 127 state agencies to provide financial information to
 128 ASSET for inclusion in a certain annual report;
 129 requiring state agencies to submit such information by
 130 a specified date annually; requiring that such
 131 information be reported to ASSET to determine all
 132 costs and expenditures of information technology
 133 assets and resources provided to state agencies;
 134 requiring ASSET to work with state agencies to provide
 135 alternative standards, policies, or requirements under
 136 specified circumstances; creating s. 282.0062, F.S.;
 137 establishing workgroups within ASSET to facilitate
 138 coordination with state agencies; providing for the
 139 membership and duties of such workgroups; creating s.
 140 282.0063, F.S.; requiring ASSET to perform specified
 141 actions to develop and manage career paths,
 142 progressions, and training programs for the benefit of
 143 state agency personnel; creating s. 282.0064, F.S.;
 144 requiring ASSET, in coordination with the Department
 145 of Management Services, to establish a policy for all

Page 5 of 107

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

576-02447-25

20257026pb

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

Page 6 of 107

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

576-02447-25

20257026pb

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

Page 7 of 107

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

576-02447-25

20257026pb

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

Page 8 of 107

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

576-02447-25

20257026pb

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

Page 9 of 107

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

576-02447-25

20257026pb

262 information security officer to establish certain
 263 guidelines and processes by a specified date;
 264 conforming cross-references; repealing s. 282.319,
 265 F.S., relating to the Florida Cybersecurity Advisory
 266 Council; establishing positions within ASSET;
 267 establishing the Division of Enterprise Information
 268 Technology Services and the Division of Enterprise
 269 Information Technology Purchasing and associated
 270 bureaus; providing the responsibilities of the
 271 bureaus; establishing the chief information officer
 272 policy workgroup; providing the membership, purpose,
 273 chair, and duties of the workgroup; providing for the
 274 expiration of the workgroup upon completion of its
 275 duties; amending s. 282.201, F.S.; revising
 276 requirements of the state data center; abrogating the
 277 scheduled repeal of the Division of Emergency
 278 Management's exemption from using the state data
 279 center; deleting Department of Management Services
 280 responsibilities related to the state data center;
 281 deleting provisions relating to contracting with the
 282 Northwest Regional Data Center; transferring,
 283 renumbering, and amending s. 1004.649, F.S.; requiring
 284 the Northwest Regional Data Center, by a specified
 285 date annually, to provide the projected costs of
 286 providing data center services for the following
 287 fiscal year to the Office of Policy and Budget in the
 288 Executive Office of the Governor and to the chairs of
 289 the legislative appropriations committees; deleting a
 290 requirement that the data center prepare and submit

Page 10 of 107

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

576-02447-25

20257026pb

291 certain invoices to the Department of Management
 292 Services for approval; conforming a cross-reference;
 293 amending s. 20.22, F.S.; deleting the Florida Digital
 294 Service from the list of divisions, programs, and
 295 services of the Department of Management Services;
 296 amending s. 282.802, F.S.; providing that the
 297 Government Technology Modernization Council is located
 298 within ASSET; providing that the state chief
 299 information officer, or his or her designee, is the ex
 300 officio executive director of the council; conforming
 301 provisions to changes made by the act; requiring the
 302 council annually to submit to the Commissioner of
 303 Agriculture, the Chief Financial Officer, and the
 304 Attorney General certain legislative recommendations;
 305 amending s. 282.604, F.S.; requiring ASSET, with input
 306 from stakeholders, to adopt rules; amending s.
 307 287.0591, F.S.; requiring the state chief information
 308 officer, instead of the Florida Digital Service, to
 309 participate in certain solicitations; amending s.
 310 288.012, F.S.; conforming a cross-reference; amending
 311 s. 443.1113, F.S.; requiring the Department of
 312 Commerce to seek input on recommended enhancements
 313 from ASSET instead of the Florida Digital Service;
 314 amending s. 943.0415, F.S.; authorizing the Cybercrime
 315 Office to consult with the state chief information
 316 security officer of ASSET instead of the Florida
 317 Digital Service; amending s. 1004.444, F.S.;
 318 authorizing the Florida Center for Cybersecurity to
 319 conduct, consult, or assist state agencies upon

Page 11 of 107

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

576-02447-25

20257026pb

320 receiving a request for assistance from such agencies;
 321 providing effective dates.
 322
 323 Be It Enacted by the Legislature of the State of Florida:
 324
 325 Section 1. Section 20.70, Florida Statutes, is created to
 326 read:
 327 20.70 Agency for State Systems and Enterprise Technology.—
 328 There is created the Agency for State Systems and Enterprise
 329 Technology. The head of the agency is the Governor and Cabinet.
 330 (1) DIVISIONS AND OFFICES.—The following divisions and
 331 offices of the Agency for State Systems and Enterprise
 332 Technology are established:
 333 (a) The Division of Administrative Services.
 334 (b) The Office of Information Technology.
 335 (c) Beginning July 1, 2026:
 336 1. The Division of Enterprise Data and Interoperability.
 337 2. The Division of Enterprise Security.
 338 3. The Division of Enterprise Information Technology
 339 Services.
 340 4. The Division of Enterprise Information Technology
 341 Purchasing.
 342 5. The Division of Enterprise Information Technology
 343 Workforce Development.
 344 (2) EXECUTIVE DIRECTOR.—The executive director of the
 345 Agency for State Systems and Enterprise Technology also serves
 346 as the state chief information officer. The Governor and Cabinet
 347 shall appoint a state chief information officer from nominees of
 348 the state chief information officer selection committee. The

Page 12 of 107

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

576-02447-25

20257026pb

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

357 (3) STATE CHIEF INFORMATION OFFICER SELECTION COMMITTEE.—

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

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

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

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

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

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

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

Page 13 of 107

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

576-02447-25

20257026pb

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

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

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

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

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

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

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

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

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

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

Page 14 of 107

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

576-02447-25

20257026pb

407 NIST, ISO 27001, and applicable federal and state security
 408 regulations;
 409 2. Cloud and digital services with experience with cloud
 410 computing, enterprise systems modernization, digital
 411 transformation, and emerging information technology trends;
 412 3. Information technology governance and policy development
 413 by demonstrating an understanding of statewide information
 414 technology governance structures, digital services, and
 415 information technology procurement policies; and
 416 4. Public sector information technology management by
 417 demonstrating familiarity with government information technology
 418 funding models, procurement requirements, and legislative
 419 processes affecting information technology strategy.
 420 (d) Leadership and administrative competencies.—The state
 421 chief information officer must demonstrate:
 422 1. Strategic vision and innovation by possessing the
 423 capability to modernize information technology systems, drive
 424 digital transformation, and align information technology
 425 initiatives with state goals;
 426 2. Collaboration and engagement with stakeholders by
 427 working with legislators, state agency heads, local governments,
 428 and private sector partners to implement information technology
 429 initiatives;
 430 3. Crisis management and cyber resilience by possessing the
 431 capability to develop and lead cyber incident response, disaster
 432 recovery, and information technology continuity plans; and
 433 4. Fiscal management and budget expertise managing multi-
 434 million-dollar information technology budgets, cost-control
 435 strategies, and financial oversight of information technology

Page 15 of 107

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

576-02447-25

20257026pb

436 projects.
 437 (e) Previous appointment or service.—A person who is
 438 currently serving or has previously served as the head of a
 439 state agency in the state is ineligible for nomination,
 440 appointment, or service as the state chief information officer.
 441 Section 2. Until a state chief information officer is
 442 appointed pursuant to s. 20.70, Florida Statutes, the current
 443 state chief information officer of the Department of Management
 444 Services shall be transferred to the Agency for State Systems
 445 and Enterprise Technology and serve as interim state chief
 446 information officer. A state chief information officer for the
 447 Agency for State Systems and Enterprise Technology must be
 448 appointed by the Governor and Cabinet by January 2, 2026.
 449 Appointments to the state chief information officer selection
 450 committee must be made by August 1, 2025.
 451 Section 3. Effective July 1, 2026, paragraph (b) of
 452 subsection (3) of section 97.0525, Florida Statutes, is amended
 453 to read:
 454 97.0525 Online voter registration.—
 455 (3)
 456 (b) The division shall conduct a comprehensive risk
 457 assessment of the online voter registration system every 2
 458 years. The comprehensive risk assessment must comply with the
 459 risk assessment methodology developed by the Agency for State
 460 Systems and Enterprise Technology ~~Department of Management~~
 461 ~~Services~~ for identifying security risks, determining the
 462 magnitude of such risks, and identifying areas that require
 463 safeguards. In addition, the comprehensive risk assessment must
 464 incorporate all of the following:

Page 16 of 107

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

576-02447-25

20257026pb

- 465 1. Load testing and stress testing to ensure that the
 466 online voter registration system has sufficient capacity to
 467 accommodate foreseeable use, including during periods of high
 468 volume of website users in the week immediately preceding the
 469 book-closing deadline for an election.
- 470 2. Screening of computers and networks used to support the
 471 online voter registration system for malware and other
 472 vulnerabilities.
- 473 3. Evaluation of database infrastructure, including
 474 software and operating systems, in order to fortify defenses
 475 against cyberattacks.
- 476 4. Identification of any anticipated threats to the
 477 security and integrity of data collected, maintained, received,
 478 or transmitted by the online voter registration system.
- 479 Section 4. Effective July 1, 2026, paragraphs (a) and (f)
 480 of subsection (1), paragraphs (b) and (c) of subsection (2), and
 481 subsections (3) and (4) of section 112.22, Florida Statutes, are
 482 amended to read:
- 483 112.22 Use of applications from foreign countries of
 484 concern prohibited.—
- 485 (1) As used in this section, the term:
- 486 (a) "ASSET" means the Agency for State Systems and
 487 Enterprise Technology "Department" means the Department of
 488 Management Services.
- 489 (f) "Prohibited application" means an application that
 490 meets the following criteria:
- 491 1. Any Internet application that is created, maintained, or
 492 owned by a foreign principal and that participates in activities
 493 that include, but are not limited to:

Page 17 of 107

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

576-02447-25

20257026pb

- 494 a. Collecting keystrokes or sensitive personal, financial,
 495 proprietary, or other business data;
- 496 b. Compromising e-mail and acting as a vector for
 497 ransomware deployment;
- 498 c. Conducting cyber-espionage against a public employer;
- 499 d. Conducting surveillance and tracking of individual
 500 users; or
- 501 e. Using algorithmic modifications to conduct
 502 disinformation or misinformation campaigns; or
- 503 2. Any Internet application ASSET ~~the department~~ deems to
 504 present a security risk in the form of unauthorized access to or
 505 temporary unavailability of the public employer's records,
 506 digital assets, systems, networks, servers, or information.
- 507 (2)
- 508 (b) A person, including an employee or officer of a public
 509 employer, may not download or access any prohibited application
 510 on any government-issued device.
- 511 1. This paragraph does not apply to a law enforcement
 512 officer as defined in s. 943.10(1) if the use of the prohibited
 513 application is necessary to protect the public safety or conduct
 514 an investigation within the scope of his or her employment.
- 515 2. A public employer may request a waiver from ASSET ~~the~~
 516 ~~department~~ to allow designated employees or officers to download
 517 or access a prohibited application on a government-issued
 518 device.
- 519 (c) Within 15 calendar days after ASSET ~~the department~~
 520 issues or updates its list of prohibited applications pursuant
 521 to paragraph (3)(a), an employee or officer of a public employer
 522 who uses a government-issued device must remove, delete, or

Page 18 of 107

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

576-02447-25

20257026pb

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

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

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

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

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

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

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

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

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

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

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

Page 19 of 107

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

576-02447-25

20257026pb

552 administer this section.

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

556 119.0725 Agency cybersecurity information; public records
557 exemption; public meetings exemption.—

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

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

567 216.023 Legislative budget requests to be furnished to
568 Legislature by agencies.—

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

Page 20 of 107

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

576-02447-25

20257026pb

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

- 584 (a) The name of the technology system.
- 585 (b) A brief description of the purpose and function of the
 586 system.
- 587 (c) A brief description of the goals of the project.
- 588 (d) The initiation date of the project.
- 589 (e) The key performance indicators for the project.
- 590 (f) Any other metrics for the project evaluating the health
 591 and status of the project.
- 592 (g) The original and current baseline estimated end dates
 593 of the project.
- 594 (h) The original and current estimated costs of the
 595 project.
- 596 (i) Total funds appropriated or allocated to the project
 597 and the current realized cost for the project by fiscal year.

598 ~~For purposes of this subsection, an ongoing technology-related~~
 599 ~~project is one which has been funded or has had or is expected~~
 600 ~~to have expenditures in more than one fiscal year. An ongoing~~
 601 ~~technology-related project does not include the continuance of~~
 602 ~~existing hardware and software maintenance agreements, the~~
 603 ~~renewal of existing software licensing agreements, or the~~
 604 ~~replacement of desktop units with new technology that is~~
 605 ~~substantially similar to the technology being replaced. This~~
 606 ~~subsection expires July 1, 2025.~~
 607
 608 Section 7. Effective July 1, 2026, paragraph (a) of
 609 subsection (4) and subsection (7) of section 216.023, Florida

Page 21 of 107

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

576-02447-25

20257026pb

610 Statutes, are amended to read:

611 216.023 Legislative budget requests to be furnished to
 612 Legislature by agencies.—

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

- 615 1. The constitutional or statutory authority for a program,
 616 a brief purpose statement, and approved program components.
- 617 2. Information on expenditures for 3 fiscal years (actual
 618 prior-year expenditures, current-year estimated expenditures,
 619 and agency budget requested expenditures for the next fiscal
 620 year) by appropriation category.
- 621 3. Details on trust funds and fees.
- 622 4. The total number of positions (authorized, fixed, and
 623 requested).
- 624 5. An issue narrative describing and justifying changes in
 625 amounts and positions requested for current and proposed
 626 programs for the next fiscal year.
- 627 6. Information resource requests.
- 628 7. Supporting information, including applicable cost-
 629 benefit analyses, business case analyses, performance
 630 contracting procedures, service comparisons, and impacts on
 631 performance standards for any request to outsource or privatize
 632 state agency functions. The cost-benefit and business case
 633 analyses must include an assessment of the impact on each
 634 affected activity from those identified in accordance with
 635 paragraph (b). Performance standards must include standards for
 636 each affected activity and be expressed in terms of the
 637 associated unit of activity.
- 638 8. An evaluation of major outsourcing and privatization

Page 22 of 107

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

576-02447-25

20257026pb

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

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

654 10. For projects that exceed \$10 million in total cost, the
 655 statutory reference of the existing policy or the proposed
 656 substantive policy that establishes and defines the project's
 657 governance structure, planned scope, main business objectives
 658 that must be achieved, and estimated completion timeframes. The
 659 governance structure for information technology-related projects
 660 must incorporate the applicable project management and oversight
 661 standards established pursuant to s. 282.0061 ~~s. 282.0051~~.

662 Information technology budget requests for the continuance of
 663 existing hardware and software maintenance agreements, renewal
 664 of existing software licensing agreements, or the replacement of
 665 desktop units with new technology that is similar to the
 666 technology currently in use are exempt from this requirement.

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

576-02447-25

20257026pb

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

- 682 ~~(a) The name of the technology system.~~
 683 ~~(b) A brief description of the purpose and function of the~~
 684 ~~system.~~
 685 ~~(c) A brief description of the goals of the project.~~
 686 ~~(d) The initiation date of the project.~~
 687 ~~(e) The key performance indicators for the project.~~
 688 ~~(f) Any other metrics for the project evaluating the health~~
 689 ~~and status of the project.~~
 690 ~~(g) The original and current baseline estimated end dates~~
 691 ~~of the project.~~
 692 ~~(h) The original and current estimated costs of the~~
 693 ~~project.~~
 694 ~~(i) Total funds appropriated or allocated to the project~~
 695 ~~and the current realized cost for the project by fiscal year.~~
 696 Section 8. Present subsections (36), (37), and (38) of

576-02447-25 20257026pb

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

701 282.0041 Definitions.—As used in this chapter, the term:

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

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

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

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

725 282.0051 Department of Management Services; Florida Digital

576-02447-25 20257026pb

726 Service; powers, duties, and functions.—

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

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

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

745 (c) Direct the state chief information security officer to
 746 provide a consolidated cybersecurity incident report by the 30th
 747 day after the end of each quarter to the interim state chief
 748 information officer, the Executive Office of the Governor, the
 749 Commissioner of Agriculture, the Chief Financial Officer, the
 750 Attorney General, the President of the Senate, and the Speaker
 751 of the House of Representatives ~~Develop and publish information~~
 752 ~~technology policy for the management of the state’s information~~
 753 ~~technology resources.~~

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

576-02447-25

20257026pb

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

758 ~~2. Supports the cloud-first policy as specified in s.~~
 759 ~~282.206; and~~

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

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

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

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

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

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

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

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

Page 27 of 107

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

576-02447-25

20257026pb

784 ~~information technology projects that have total project costs of~~
 785 ~~\$10 million or more and that are funded in the General~~
 786 ~~Appropriations Act or any other law. The department, acting~~
 787 ~~through the Florida Digital Service, shall report at least~~
 788 ~~quarterly to the Executive Office of the Governor, the President~~
 789 ~~of the Senate, and the Speaker of the House of Representatives~~
 790 ~~on any information technology project that the department~~
 791 ~~identifies as high-risk due to the project exceeding acceptable~~
 792 ~~variance ranges defined and documented in a project plan. The~~
 793 ~~report must include a risk assessment, including fiscal risks,~~
 794 ~~associated with proceeding to the next stage of the project, and~~
 795 ~~a recommendation for corrective actions required, including~~
 796 ~~suspension or termination of the project.~~

797 ~~(c) Identify opportunities for standardization and~~
 798 ~~consolidation of information technology services that support~~
 799 ~~interoperability and the cloud-first policy, as specified in s.~~
 800 ~~282.206, and business functions and operations, including~~
 801 ~~administrative functions such as purchasing, accounting and~~
 802 ~~reporting, cash management, and personnel, and that are common~~
 803 ~~across state agencies. The department, acting through the~~
 804 ~~Florida Digital Service, shall biennially on January 1 of each~~
 805 ~~even-numbered year provide recommendations for standardization~~
 806 ~~and consolidation to the Executive Office of the Governor, the~~
 807 ~~President of the Senate, and the Speaker of the House of~~
 808 ~~Representatives.~~

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

Page 28 of 107

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

576-02447-25

20257026pb

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

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

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

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

Page 29 of 107

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

576-02447-25

20257026pb

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

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

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

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

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

Page 30 of 107

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

576-02447-25

20257026pb

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

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

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

Page 31 of 107

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

576-02447-25

20257026pb

900 ~~(p)1. Establish an information technology policy for all~~
 901 ~~information technology-related state contracts, including state~~
 902 ~~term contracts for information technology commodities,~~
 903 ~~consultant services, and staff augmentation services. The~~
 904 ~~information technology policy must include:~~
 905 ~~a. Identification of the information technology product and~~
 906 ~~service categories to be included in state term contracts.~~
 907 ~~b. Requirements to be included in solicitations for state~~
 908 ~~term contracts.~~
 909 ~~c. Evaluation criteria for the award of information~~
 910 ~~technology-related state term contracts.~~
 911 ~~d. The term of each information technology related state~~
 912 ~~term contract.~~
 913 ~~e. The maximum number of vendors authorized on each state~~
 914 ~~term contract.~~
 915 ~~f. At a minimum, a requirement that any contract for~~
 916 ~~information technology commodities or services meet the National~~
 917 ~~Institute of Standards and Technology Cybersecurity Framework.~~
 918 ~~g. For an information technology project wherein project~~
 919 ~~oversight is required pursuant to paragraph (d) or paragraph~~
 920 ~~(m), a requirement that independent verification and validation~~
 921 ~~be employed throughout the project life cycle with the primary~~
 922 ~~objective of independent verification and validation being to~~
 923 ~~provide an objective assessment of products and processes~~
 924 ~~throughout the project life cycle. An entity providing~~
 925 ~~independent verification and validation may not have technical,~~
 926 ~~managerial, or financial interest in the project and may not~~
 927 ~~have responsibility for, or participate in, any other aspect of~~
 928 ~~the project.~~

Page 32 of 107

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

576-02447-25

20257026pb

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

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

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

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

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

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

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

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

Page 33 of 107

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

576-02447-25

20257026pb

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

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

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

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

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

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

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

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

Page 34 of 107

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

576-02447-25

20257026pb

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

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

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

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

998 ~~(a) State agencies must provide the Florida Digital Service~~
 999 ~~with written notice of any planned procurement of an information~~
 1000 ~~technology project.~~

1001 ~~(b) The Florida Digital Service must participate in the~~
 1002 ~~development of specifications and recommend modifications to any~~
 1003 ~~planned procurement of an information technology project by~~
 1004 ~~state agencies so that the procurement complies with the~~
 1005 ~~enterprise architecture.~~

1006 ~~(c) The Florida Digital Service must participate in post-~~
 1007 ~~award contract monitoring.~~

1008 ~~(2)(5)~~ The department, acting through the Florida Digital
 1009 Service, may not retrieve or disclose any data without a shared-
 1010 data agreement in place between the department and the
 1011 enterprise entity that has primary custodial responsibility of,
 1012 or data-sharing responsibility for, that data.

1013 (3) This section is repealed July 1, 2026.

1014 ~~(6) The department, acting through the Florida Digital~~
 1015 ~~Service, shall adopt rules to administer this section.~~

Page 35 of 107

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

576-02447-25

20257026pb

1016 Section 10. Section 282.00515, Florida Statutes, is
 1017 repealed.

1018 Section 11. Effective July 1, 2026, section 282.006,
 1019 Florida Statutes, is created to read:

1020 282.006 Agency for State Systems and Enterprise Technology;
 1021 duties; enterprise responsibilities; reporting.-

1022 (1) The Agency for State Systems and Enterprise Technology
 1023 established in s. 20.70 shall operate as the state enterprise
 1024 organization for information technology governance and is the
 1025 lead entity responsible for understanding the unique state
 1026 agency information technology needs and environments, creating
 1027 enterprise technology standards and strategy, supporting state
 1028 agency technology efforts, and reporting on the status of
 1029 technology for the enterprise.

1030 (2) The Legislature intends for ASSET policy, standards,
 1031 guidance, and oversight to allow for adaptability to emerging
 1032 technology and organizational needs while maintaining compliance
 1033 with industry best practices. All policies, standards, and
 1034 guidelines established pursuant to this chapter must be
 1035 technology-agnostic and may not prescribe specific tools,
 1036 platforms, or vendors.

1037 (3) ASSET shall establish the strategic direction of
 1038 information technology in the state. ASSET shall develop and
 1039 publish information technology policy that aligns with industry
 1040 best practices for the management of the state's information
 1041 technology resources. The policy must be updated as necessary to
 1042 meet the requirements of this chapter and advancements in
 1043 technology.

1044 (4) Related to its oversight of the state's technology

Page 36 of 107

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

576-02447-25

20257026pb

1045 enterprise, ASSET shall:

1046 (a) In coordination with state agency technology subject

1047 matter experts, develop, publish, and maintain an enterprise

1048 architecture that:

1049 1. Acknowledges the unique needs of the entities within the

1050 enterprise in the development and publication of standards and

1051 terminologies to facilitate digital interoperability;

1052 2. Supports the cloud-first policy as specified in s.

1053 282.206;

1054 3. Addresses how information technology infrastructure may

1055 be modernized to achieve security, scalability, maintainability,

1056 interoperability, and improved cost-efficiency goals; and

1057 4. Includes, at a minimum, best practices, guidelines, and

1058 standards for:

1059 a. Data models and taxonomies.

1060 b. Master data management.

1061 c. Data integration and interoperability.

1062 d. Data security and encryption.

1063 e. Bot prevention and data protection.

1064 f. Data backup and recovery.

1065 g. Application portfolio and catalog requirements.

1066 h. Application architectural patterns and principles.

1067 i. Technology and platform standards.

1068 j. Secure coding practices.

1069 k. Performance and scalability.

1070 l. Cloud infrastructure and architecture.

1071 m. Networking, connectivity, and security protocols.

1072 n. Authentication, authorization, and access controls.

1073 o. Disaster recovery.

Page 37 of 107

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

576-02447-25

20257026pb

1074 p. Quality assurance.

1075 g. Testing methodologies and measurements.

1076 r. Logging and log retention.

1077 s. Application and use of artificial intelligence.

1078 (b) Recommend open data technical standards and

1079 terminologies for use by the state's technology enterprise.

1080 (c) Develop enterprise technology testing and quality

1081 assurance best practices and standards to ensure the

1082 reliability, security, and performance of information technology

1083 systems. Such best practices and standards must include:

1084 1. Functional testing to ensure software or systems meet

1085 required specifications.

1086 2. Performance and load testing to ensure software and

1087 systems operate efficiently under various conditions.

1088 3. Security testing to protect software and systems from

1089 vulnerabilities and cyber threats.

1090 4. Compatibility and interoperability testing to ensure

1091 software and systems operate seamlessly across environments.

1092 (5) ASSET shall produce the following reports and provide

1093 them to the Governor, the Commissioner of Agriculture, the Chief

1094 Financial Officer, the Attorney General, the President of the

1095 Senate, and the Speaker of the House of Representatives:

1096 (a) Annually by December 15, an enterprise analysis report

1097 that includes all of the following:

1098 1. Results of the state agency needs assessments, including

1099 any plan to address technical debt as required by s. 282.0061

1100 pursuant to the schedule adopted.

1101 2. Alternative standards related to federal funding adopted

1102 pursuant to s. 282.0061.

Page 38 of 107

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

576-02447-25

20257026pb

1103 3. Information technology financial data for each state
 1104 agency for the previous fiscal year. This portion of the annual
 1105 report must include, at a minimum, the following recurring and
 1106 nonrecurring information:

1107 a. Total number of full-time equivalent positions.
 1108 b. Total amount of salary.
 1109 c. Total amount of benefits.
 1110 d. Total number of comparable full-time equivalent
 1111 positions and total amount of expenditures for information
 1112 technology staff augmentation.

1113 e. Total number of contracts and purchase orders and total
 1114 amount of associated expenditures for information technology
 1115 managed services.

1116 f. Total amount of expenditures by state term contract as
 1117 defined in s. 287.012, contracts procured using alternative
 1118 purchasing methods as authorized pursuant to s. 287.042(16), and
 1119 state agency procurements through request for proposal,
 1120 invitation to negotiate, invitation to bid, single source, and
 1121 emergency purchases.

1122 g. Total amount of expenditures for hardware.
 1123 h. Total amount of expenditures for non-cloud software.
 1124 i. Total amount of expenditures for cloud software licenses
 1125 and services with a separate amount for expenditures for state
 1126 data center services.

1127 j. Total amount of expenditures for cloud data center
 1128 services with a separate amount for expenditures for state data
 1129 center services.

1130 k. Total amount of expenditures for administrative costs.
 1131 4. Consolidated information for the previous fiscal year

Page 39 of 107

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

576-02447-25

20257026pb

1132 about state information technology projects, which must include,
 1133 at a minimum, the following information:

1134 a. Anticipated funding requirements for information
 1135 technology support over the next 5 years.

1136 b. An inventory of current information technology assets
 1137 and major projects. The term "major project" includes projects
 1138 costing more than \$500,000 to implement.

1139 c. Significant unmet needs for information technology
 1140 resources over the next 5 fiscal years, ranked in priority order
 1141 according to their urgency.

1142 5. A review and summary of whether the information
 1143 technology contract policy established pursuant to s. 282.0064
 1144 is included in all solicitations and contracts.

1145 6. Information related to the information technology test
 1146 laboratory created in s. 282.0065, including usage statistics
 1147 and key findings, and recommendations for improving the state's
 1148 information technology procurement processes.

1149 (b) Biennially by December 15 of even-numbered years, a
 1150 report on the strategic direction of information technology in
 1151 the state which includes all of the following:

1152 1. Recommendations for standardization and consolidation of
 1153 information technology services that are identified as common
 1154 across state agencies as required in s. 282.0061.

1155 2. Recommendations for information technology services that
 1156 should be designed, delivered, and managed as enterprise
 1157 information technology services. Recommendations must include
 1158 the identification of existing information technology resources
 1159 associated with the services, if existing services must be
 1160 transferred as a result of being delivered and managed as

Page 40 of 107

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

576-02447-25

20257026pb

1161 enterprise information technology services, and which entity is
 1162 best suited to manage the service.

1163 (c)1. When conducted as provided in this paragraph, a
 1164 market analysis and accompanying strategic plan submitted by
 1165 December 31 of each year that the market analysis is conducted.

1166 2. No less frequently than every 3 years, ASSET shall
 1167 conduct market analysis to determine whether the:

1168 a. Information technology resources within the enterprise
 1169 are used in the most cost-effective and cost-efficient manner,
 1170 while recognizing that the replacement of certain legacy
 1171 information technology systems within the enterprise may be cost
 1172 prohibitive or cost inefficient due to the remaining useful life
 1173 of those resources; and

1174 b. Enterprise is using best practices with respect to
 1175 information technology, information services, and the
 1176 acquisition of emerging technologies and information services.

1177 3. Each market analysis must be used to prepare a strategic
 1178 plan for continued and future information technology and
 1179 information services for the enterprise, including, but not
 1180 limited to, proposed acquisition of new services or technologies
 1181 and approaches to the implementation of any new services or
 1182 technologies.

1183 (6) ASSET may adopt rules to implement this chapter.

1184 Section 12. Effective July 1, 2026, section 282.0061,
 1185 Florida Statutes, is created to read:

1186 282.0061 ASSET support of state agencies; information
 1187 technology procurement and projects.-

1188 (1) LEGISLATIVE INTENT.-The Legislature intends for ASSET
 1189 to support state agencies in their information technology

576-02447-25

20257026pb

1190 efforts through the adoption of policies, standards, and
 1191 guidance and by providing oversight that recognizes unique state
 1192 agency information technology needs, environments, and goals.
 1193 ASSET assistance and support must allow for adaptability to
 1194 emerging technologies and organizational needs while maintaining
 1195 compliance with industry best practices. ASSET may not prescribe
 1196 specific tools, platforms, or vendors.

1197 (2) NEEDS ASSESSMENTS.-

1198 (a) By January 1, 2028, ASSET shall conduct full baseline
 1199 needs assessments of state agencies to document their distinct
 1200 technical environments, existing technical debt, security risks,
 1201 and compliance with all information technology standards and
 1202 guidelines developed and published by ASSET. The needs
 1203 assessment must use the Capability Maturity Model to evaluate
 1204 each state agency's information technology capabilities,
 1205 providing a maturity level rating for each assessed domain.
 1206 After completion of the full baseline needs assessments, such
 1207 assessments must be maintained and updated on a regular schedule
 1208 adopted by ASSET.

1209 (b) In assessing the existing technical debt portion of the
 1210 needs assessment, ASSET shall analyze the state's legacy
 1211 information technology systems and develop a plan to document
 1212 the needs and costs for replacement systems. The plan must
 1213 include an inventory of legacy applications and infrastructure;
 1214 the required capabilities not available with the legacy system;
 1215 the estimated process, timeline, and cost to migrate from legacy
 1216 environments; and any other information necessary for fiscal or
 1217 technology planning. The plan must determine and document the
 1218 estimated timeframe during which the state agency can continue

576-02447-25

20257026pb

1219 to efficiently use legacy information technology systems,
 1220 resources, security, and data management to support operations.
 1221 State agencies shall provide all necessary documentation to
 1222 enable accurate reporting on legacy systems.

1223 (c) ASSET shall develop a plan and schedule to conduct the
 1224 initial full baseline needs assessments. By October 1, 2026,
 1225 ASSET shall submit the plan to the Governor, the Commissioner of
 1226 Agriculture, the Chief Financial Officer, the Attorney General,
 1227 the President of the Senate, and the Speaker of the House of
 1228 Representatives.

1229 (d) ASSET shall support state agency strategic planning
 1230 efforts and assist state agencies with the production of a
 1231 phased roadmap to address known technology gaps and deficiencies
 1232 as identified in the needs assessments. The roadmaps must
 1233 include specific strategies and initiatives aimed at advancing
 1234 the state agency's maturity level in accordance with the
 1235 Capability Maturity Model. State agencies shall create,
 1236 maintain, and submit the roadmap on an annual basis with their
 1237 legislative budget requests required under s. 216.023.

1238 (3) STANDARDIZATION.—ASSET shall:

1239 (a) Recommend in its annual enterprise analysis required
 1240 under s. 282.006 any potential methods for standardizing data
 1241 across state agencies which will promote interoperability and
 1242 reduce the collection of duplicative data.

1243 (b) Identify any opportunities in its annual enterprise
 1244 analysis required under s. 282.006 for standardization and
 1245 consolidation of information technology services that are common
 1246 across all state agencies and that support:

1247 1. Improved interoperability, security, scalability,

Page 43 of 107

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

576-02447-25

20257026pb

1248 maintainability, and cost efficiency; and

1249 2. Business functions and operations, including
 1250 administrative functions such as purchasing, accounting and
 1251 reporting, cash management, and personnel.

1252 (4) DATA MANAGEMENT.—

1253 (a) ASSET shall develop standards for use by state agencies
 1254 which support best practices for master data management at the
 1255 state agency level to facilitate enterprise data sharing and
 1256 interoperability.

1257 (b) ASSET shall establish a methodology and strategy for
 1258 implementing statewide master data management and submit a
 1259 report to the Governor, the Commissioner of Agriculture, the
 1260 Chief Financial Officer, the Attorney General, the President of
 1261 the Senate, and the Speaker of the House of Representatives by
 1262 December 1, 2028. The report must include the vision, goals, and
 1263 benefits of implementing a statewide master data management
 1264 initiative, an analysis of the current state of data management,
 1265 and the recommended strategy, methodology, and estimated
 1266 timeline and resources needed at a state agency and enterprise
 1267 level to accomplish the initiative.

1268 (5) INFORMATION TECHNOLOGY PROJECTS.—ASSET has the
 1269 following duties and responsibilities related to state agency
 1270 technology projects:

1271 (a) Provide procurement advisory and review services for
 1272 information technology projects to all state agencies, including
 1273 procurement and contract development assistance to meet the
 1274 information technology contract policy established pursuant to
 1275 s. 282.0064.

1276 (b) Establish best practices and enterprise procurement

Page 44 of 107

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

576-02447-25

20257026pb

1277 processes and develop metrics to support these processes for the
 1278 procurement of information technology products and services in
 1279 order to reduce costs or improve the provision of government
 1280 services.

1281 (c) Upon request, assist state agencies in the development
 1282 of information technology-related legislative budget requests.

1283 (d) Develop standards and accountability measures for
 1284 information technology projects, including criteria for
 1285 effective project management and oversight. State agencies must
 1286 satisfy these standards and measures when implementing
 1287 information technology projects. To support data-driven
 1288 decisionmaking, the standards and measures must include, but are
 1289 not limited to:

1290 1. Performance measurements and metrics that objectively
 1291 reflect the status of an information technology project based on
 1292 a defined and documented project scope, to include the volume of
 1293 impacted stakeholders, cost, and schedule.

1294 2. Methodologies for calculating and defining acceptable
 1295 variances in the projected versus actual scope, schedule, or
 1296 cost of an information technology project.

1297 3. Reporting requirements designed to alert all defined
 1298 stakeholders that an information technology project has exceeded
 1299 acceptable variances defined and documented in a project plan as
 1300 well as any variances that represent a schedule delay of 1 month
 1301 or more or a cost increase of \$1 million or more.

1302 4. Technical standards to ensure an information technology
 1303 project complies with the enterprise architecture standards.

1304 (e) Develop information technology project reports for use
 1305 by state agencies, including, but not limited to, operational

Page 45 of 107

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

576-02447-25

20257026pb

1306 work plans, project spending plans, and project status reports.
 1307 Reporting standards must include content, format, and frequency
 1308 of project updates.

1309 (f) Provide training opportunities to state agencies to
 1310 assist in the adoption of the project management and oversight
 1311 standards.

1312 (g) Perform project oversight on all state agency
 1313 information technology projects that have total project costs of
 1314 \$10 million or more. ASSET shall report by the 30th day after
 1315 the end of each quarter to the Executive Office of the Governor,
 1316 the Commissioner of Agriculture, the Chief Financial Officer,
 1317 the Attorney General, the President of the Senate, and the
 1318 Speaker of the House of Representatives on any information
 1319 technology project that ASSET identifies as high-risk. The
 1320 report must include a risk assessment, including fiscal risks,
 1321 associated with proceeding to the next stage of the project, and
 1322 a recommendation for corrective actions required, including
 1323 suspension or termination of the project.

1324 (6) INFORMATION TECHNOLOGY FINANCIAL DATA.—

1325 (a) In consultation with state agencies, ASSET shall create
 1326 a methodology, an approach, and applicable templates and formats
 1327 for identifying and collecting both current and planned
 1328 information technology expenditure data at the state agency
 1329 level. ASSET shall continuously obtain, review, and maintain
 1330 records of the appropriations, expenditures, and revenues for
 1331 information technology for each state agency.

1332 (b) ASSET shall prescribe the format for state agencies to
 1333 provide all necessary financial information to ASSET for
 1334 inclusion in the annual report required under s. 282.006. State

Page 46 of 107

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

576-02447-25

20257026pb

1335 agencies must provide the information to ASSET by October 1 for
 1336 the previous fiscal year. The information must be reported by
 1337 ASSET in order to determine all costs and expenditures for
 1338 information technology assets and resources provided by the
 1339 state agencies or through contracts or grants.

1340 (7) FEDERAL CONFLICTS.—ASSET shall work with state agencies
 1341 to provide alternative standards, policies, or requirements that
 1342 do not conflict with federal regulations or requirements, if
 1343 adherence to standards or policies adopted by or established
 1344 pursuant to this section conflict with federal regulations or
 1345 requirements imposed on an entity within the enterprise and
 1346 results in, or is expected to result in, adverse action against
 1347 the state agencies or loss of federal funding.

1348 Section 13. Effective July 1, 2026, section 282.0062,
 1349 Florida Statutes, is created to read:

1350 282.0062 ASSET workgroups.—The following workgroups are
 1351 established within ASSET to facilitate coordination with state
 1352 agencies:

1353 (1) CHIEF INFORMATION OFFICER WORKGROUP.—

1354 (a) The chief information officer workgroup, composed of
 1355 all state agency chief information officers, shall consider and
 1356 make recommendations to the state chief information officer and
 1357 the state chief information architect on such matters as
 1358 enterprise information technology policies, standards, services,
 1359 and architecture. The workgroup may also identify and recommend
 1360 opportunities for the establishment of public-private
 1361 partnerships when considering technology infrastructure and
 1362 services in order to accelerate project delivery and provide a
 1363 source of new or increased project funding.

Page 47 of 107

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

576-02447-25

20257026pb

1364 (b) At a minimum, the state chief information officer shall
 1365 consult with the workgroup on a quarterly basis with regard to
 1366 executing the duties and responsibilities of the state agencies
 1367 related to statewide information technology strategic planning
 1368 and policy.

1369 (2) ENTERPRISE DATA AND INTEROPERABILITY WORKGROUP.—

1370 (a) The enterprise data and interoperability workgroup,
 1371 composed of chief data officer representatives from all state
 1372 agencies, shall consider and make recommendations to the state
 1373 chief data officer on such matters as enterprise data policies,
 1374 standards, services, and architecture that promote data
 1375 consistency, accessibility, and seamless integration across the
 1376 enterprise.

1377 (b) At a minimum, the state chief data officer shall
 1378 consult with the workgroup on a quarterly basis with regard to
 1379 executing the duties and responsibilities of the state agencies
 1380 related to statewide data governance planning and policy.

1381 (3) ENTERPRISE SECURITY WORKGROUP.—

1382 (a) The enterprise security workgroup, composed of chief
 1383 security officer representatives from all state agencies, shall
 1384 consider and make recommendations to the state chief security
 1385 officer on such matters as cybersecurity policies, standards,
 1386 services, and architecture that promote the protection of state
 1387 assets.

1388 (b) At a minimum, the state chief security officer shall
 1389 consult with the workgroup on a quarterly basis with regard to
 1390 executing the duties and responsibilities of the state agencies
 1391 related to cybersecurity governance and policy development.

1392 (4) ENTERPRISE INFORMATION TECHNOLOGY OPERATIONS

Page 48 of 107

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

576-02447-25

20257026pb

1393 WORKGROUP.-

1394 (a) The enterprise information technology operations
 1395 workgroup, composed of information technology business analyst
 1396 representatives from all state agencies, shall consider and make
 1397 recommendations to the state chief technology officer on such
 1398 matters as information technology needs assessments policies,
 1399 standards, and services that promote the strategic alignment of
 1400 technology with operational needs and the evaluation of
 1401 solutions across the enterprise.

1402 (b) At a minimum, the state chief technology officer shall
 1403 consult with the workgroup on a quarterly basis with regard to
 1404 executing the duties and responsibilities of the state agencies
 1405 related to statewide process improvement and optimization.

1406 (5) ENTERPRISE INFORMATION TECHNOLOGY QUALITY ASSURANCE
 1407 WORKGROUP.-

1408 (a) The enterprise information technology quality assurance
 1409 workgroup, composed of testing and quality assurance
 1410 representatives from all state agencies, shall consider and make
 1411 recommendations to the state chief technology officer on such
 1412 matters as testing methodologies, tools, and best practices to
 1413 reduce risks related to software defects, cybersecurity threats,
 1414 and operational failures.

1415 (b) At a minimum, the state chief technology officer shall
 1416 consult with the workgroup on a quarterly basis with regard to
 1417 executing the duties and responsibilities of the state agencies
 1418 related to enterprise software testing and quality assurance
 1419 standards.

1420 (6) ENTERPRISE INFORMATION TECHNOLOGY PROJECT MANAGEMENT
 1421 WORKGROUP.-

Page 49 of 107

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

576-02447-25

20257026pb

1422 (a) The enterprise information technology project
 1423 management workgroup, composed of information technology project
 1424 manager representatives from all state agencies, shall consider
 1425 and make recommendations to the state chief technology officer
 1426 on such matters as information technology project management
 1427 policies, standards, accountability measures, and services that
 1428 promote project governance and standardization across the
 1429 enterprise.

1430 (b) At a minimum, the state chief technology officer shall
 1431 consult with the workgroup on a quarterly basis with regard to
 1432 executing the duties and responsibilities of the state agencies
 1433 related to project management and oversight.

1434 (7) ENTERPRISE INFORMATION TECHNOLOGY CONTRACT MANAGEMENT
 1435 WORKGROUP.-

1436 (a) The enterprise information technology contract
 1437 management workgroup, composed of information technology
 1438 contract manager representatives from all state agencies, shall
 1439 consider and make recommendations to the state chief technology
 1440 officer on such matters as information technology contract
 1441 management policies and standards that promote best practices
 1442 for vendor oversight, risk management and compliance, and
 1443 performance monitoring and reporting across the enterprise.

1444 (b) At a minimum, the state chief technology officer shall
 1445 consult with the workgroup on a quarterly basis with regard to
 1446 executing the duties and responsibilities of the state agencies
 1447 related to contract management and vendor accountability.

1448 (8) ENTERPRISE INFORMATION TECHNOLOGY PURCHASING
 1449 WORKGROUP.-

1450 (a) The enterprise information technology purchasing

Page 50 of 107

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

576-02447-25

20257026pb

1451 workgroup, composed of information technology procurement
 1452 representatives from all state agencies, shall consider and make
 1453 recommendations to the state chief technology procurement
 1454 officer on such matters as information technology procurement
 1455 policies, standards, and purchasing strategy and optimization
 1456 that promote best practices for contract negotiation,
 1457 consolidation, and effective service-level agreement
 1458 implementation across the enterprise.

1459 (b) At a minimum, the state chief technology procurement
 1460 officer shall consult with the workgroup on a quarterly basis
 1461 with regard to executing the duties and responsibilities of the
 1462 state agencies related to technology evaluation, purchasing, and
 1463 cost savings.

1464 Section 14. Effective July 1, 2026, section 282.0063,
 1465 Florida Statutes, is created to read:

1466 282.0063 State information technology professionals career
 1467 paths and training.—

1468 (1) ASSET shall develop standardized frameworks for, and
 1469 career paths, progressions, and training programs for, the
 1470 benefit of state agency information technology personnel. To
 1471 meet that goal, ASSET shall:

1472 (a) Assess current and future information technology
 1473 workforce needs across state agencies, identifying skill gaps
 1474 and developing strategies to address them.

1475 (b) Develop and establish a training program for state
 1476 agencies to support the understanding and implementation of each
 1477 element of the enterprise architecture.

1478 (c) Establish training programs, certifications, and
 1479 continuing education opportunities to enhance information

Page 51 of 107

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

576-02447-25

20257026pb

1480 technology competencies, including cybersecurity, cloud
 1481 computing, and emerging technologies.

1482 (d) Support initiatives to upskill existing employees in
 1483 emerging technologies and automation, ensuring state agencies
 1484 remain competitive and innovative.

1485 (e) Develop strategies to recruit and retain information
 1486 technology professionals, including internship programs,
 1487 partnerships with educational institutions, scholarships for
 1488 service, and initiatives to attract diverse talent.

1489 (2) ASSET shall consult with CareerSource Florida, Inc.,
 1490 the Department of Commerce, and the Department of Education in
 1491 the implementation of this section.

1492 (3) Specifically, in consultation with the Division of
 1493 State Human Resource Management in the Department of Management
 1494 Services, ASSET shall:

1495 (a) Define career progression frameworks for information
 1496 technology personnel, for supporting leadership development, and
 1497 for providing mentorship programs.

1498 (b) Establish guidelines and best practices for information
 1499 technology professional development and performance management
 1500 across state agencies.

1501 Section 15. Effective July 1, 2026, section 282.0064,
 1502 Florida Statutes, is created to read:

1503 282.0064 Information technology contract policy.—

1504 (1) In coordination with the Department of Management
 1505 Services, ASSET shall establish a policy for all information
 1506 technology-related solicitations and contracts, including state
 1507 term contracts; contracts sourced using alternative purchasing
 1508 methods as authorized pursuant to s. 287.042(16); sole source

Page 52 of 107

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

576-02447-25

20257026pb

1509 and emergency procurements; and contracts for commodities,
 1510 consultant services, and staff augmentation services.
 1511 (2) Related to state term contracts, the information
 1512 technology policy must include:
 1513 (a) Identification of the information technology product
 1514 and service categories to be included in state term contracts.
 1515 (b) The term of each information technology-related state
 1516 term contract.
 1517 (c) The maximum number of vendors authorized on each state
 1518 term contract.
 1519 (3) For all contracts, the information technology policy
 1520 must include:
 1521 (a) Evaluation criteria for the award of information
 1522 technology-related contracts.
 1523 (b) Requirements to be included in solicitations.
 1524 (c) At a minimum, a requirement that any contract for
 1525 information technology commodities or services must meet the
 1526 requirements of the enterprise architecture and National
 1527 Institute of Standards and Technology Cybersecurity Framework.
 1528 (4) The policy must include the following requirements for
 1529 any information technology project that requires project
 1530 oversight through independent verification and validation:
 1531 (a) An entity providing independent verification and
 1532 validation may not have any:
 1533 1. Technical, managerial, or financial interest in the
 1534 project; or
 1535 2. Responsibility for or participation in any other aspect
 1536 of the project.
 1537 (b) The primary objective of independent verification and

Page 53 of 107

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

576-02447-25

20257026pb

1538 validation must be to provide an objective assessment throughout
 1539 the entire project life cycle, reporting directly to all
 1540 relevant stakeholders. An independent verification and
 1541 validation entity shall independently verify and validate
 1542 whether:
 1543 1. The project is being built and implemented in accordance
 1544 with defined technical architecture, specifications, and
 1545 requirements.
 1546 2. The project is adhering to established project
 1547 management processes.
 1548 3. The procurement of products, tools, and services and
 1549 resulting contracts align with current statutory and regulatory
 1550 requirements.
 1551 4. The value of services delivered is commensurate with
 1552 project costs.
 1553 5. The completed project meets the actual needs of the
 1554 intended users.
 1555 (c) The entity performing independent verification and
 1556 validation shall provide regular reports and assessments
 1557 directly to the designated oversight body, identifying risks,
 1558 deficiencies, and recommendations for corrective actions to
 1559 ensure project success and compliance with statutory
 1560 requirements.
 1561 (5) The Division of State Purchasing in the Department of
 1562 Management Services shall coordinate with ASSET on state term
 1563 contract solicitations and invitations to negotiate related to
 1564 information technology. ASSET shall evaluate vendor responses
 1565 and answer vendor questions on such solicitations or invitations
 1566 to negotiate.

Page 54 of 107

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

576-02447-25

20257026pb

1567 Section 16. Effective July 1, 2026, section 282.0065,
 1568 Florida Statutes, is created to read:
 1569 282.0065 ASSET information technology test laboratory.—
 1570 (1) Beginning July 1, 2027, or after all elements of the
 1571 enterprise architecture are published, whichever is later, and
 1572 subject to specific appropriation, ASSET shall establish,
 1573 maintain, and manage an information technology test laboratory
 1574 to support state agencies in evaluating information technology
 1575 services, software, and tools before procurement and
 1576 implementation.
 1577 (2) The purpose of the information technology test
 1578 laboratory is to:
 1579 (a) Serve as an independent environment for state agencies
 1580 to develop, test, and refine proofs of concept for information
 1581 technology solutions to assess functionality, security,
 1582 interoperability, and performance; and
 1583 (b) Assist state agencies in defining and improving
 1584 procurement requirements based on real-world testing and
 1585 evaluation.
 1586 (3) ASSET shall:
 1587 (a) Operate and maintain the test laboratory and ensure
 1588 that it remains fully operational with the necessary
 1589 infrastructure, resources, and security controls to support
 1590 state agency testing activities.
 1591 (b) Facilitate proofs of concept for state agencies by
 1592 providing the agencies with controlled environments to assess
 1593 emerging technologies, validate vendor claims, and conduct
 1594 comparative evaluations of information technology solutions.
 1595 (c) Support the development of requirements for state

Page 55 of 107

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

576-02447-25

20257026pb

1596 agency information technology projects by assisting state
 1597 agencies in refining technical specifications, performance
 1598 benchmarks, and security requirements prior to issuing
 1599 procurement solicitations.
 1600 (d) Ensure the security and compliance of the test
 1601 laboratory by implementing safeguards to protect sensitive data,
 1602 ensure compliance with applicable laws, and prevent unauthorized
 1603 access to testing environments.
 1604 (e) Provide access to emerging technologies by partnering
 1605 with industry and research institutions to ensure that state
 1606 agencies have the opportunity to evaluate the latest information
 1607 technology innovations relevant to government operations.
 1608 (f) Enter into partnerships with public and private
 1609 entities to support the information technology test laboratory's
 1610 operations, provided that such partnerships comply with
 1611 conflict-of-interest policies and procurement regulations.
 1612 (g) Establish policies, procedures, and eligibility
 1613 criteria for state agencies to access and use the lab.
 1614 Section 17. Section 282.0066, Florida Statutes, is created
 1615 to read:
 1616 282.0066 Enterprise Information Technology Library.—
 1617 (1) ASSET shall develop, implement, and maintain a library
 1618 to serve as the official repository for all enterprise
 1619 information technology policies, standards, guidelines, and best
 1620 practices applicable to state agencies. The library must be
 1621 online and accessible by all state agencies through a secure
 1622 authentication system.
 1623 (2) In developing the library, ASSET shall create a
 1624 structured index and search functionality to facilitate

Page 56 of 107

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

576-02447-25

20257026pb

1625 efficient retrieval of information and maintain version control
 1626 and revision history for all published documents.

1627 (3) The library must include standardized checklists
 1628 organized by technical subject areas to assist state agencies in
 1629 measuring compliance with the information technology policies,
 1630 standards, guidelines, and best practices.

1631 (4) ASSET shall establish procedures to ensure the
 1632 integrity, security, and availability of the library, including
 1633 appropriate access controls, encryption, and disaster recovery
 1634 measures. ASSET must regularly update documents and materials of
 1635 the library to reflect current state and federal requirements,
 1636 industry best practices, and emerging technologies.

1637 (5)(a) All state agencies shall reference and adhere to the
 1638 policies, standards, guidelines, and best practices contained in
 1639 the online library in information technology planning,
 1640 procurement, implementation, and operations. ASSET shall create
 1641 mechanisms for state agencies to submit feedback, request
 1642 clarifications, and recommend updates.

1643 (b)1. A state agency may request an exemption to a specific
 1644 policy, standard, or guideline when compliance is not
 1645 technically feasible, would cause undue hardship, or conflicts
 1646 with agency specific statutory requirements. The state agency
 1647 requesting an exception must submit a formal justification to
 1648 ASSET detailing all of the following:

1649 a. The specific requirement for which an exemption is
 1650 sought.

1651 b. The reason compliance is not feasible or practical.

1652 c. Any compensating controls or alternative measures the
 1653 state agency will implement to mitigate associated risks.

Page 57 of 107

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

576-02447-25

20257026pb

1654 d. The anticipated duration of the exemption.

1655 2. ASSET shall review all exemption requests and provide a
 1656 recommendation to the state chief information officer who shall
 1657 present the compliance exemption requests to the chief
 1658 information officer workgroup. Approval of exemption requests
 1659 must be made by a majority vote of the workgroup. Approved
 1660 exemptions must be documented, including conditions and
 1661 expiration dates.

1662 3. A state agency with an approved exemption must undergo
 1663 periodic review to determine whether the exemption remains
 1664 necessary or if compliance can be achieved.

1665 Section 18. Paragraphs (b), (c), (g), (h), and (i) of
 1666 subsection (3) and paragraphs (b), (c), (d), and (j) of
 1667 subsection (4) of section 282.318, Florida Statutes, are amended
 1668 to read:

1669 282.318 Cybersecurity.—

1670 (3) The department, acting through the Florida Digital
 1671 Service, is the lead entity responsible for establishing
 1672 standards and processes for assessing state agency cybersecurity
 1673 risks and determining appropriate security measures. Such
 1674 standards and processes must be consistent with generally
 1675 accepted technology best practices, including the National
 1676 Institute for Standards and Technology Cybersecurity Framework,
 1677 for cybersecurity. The department, acting through the Florida
 1678 Digital Service, shall adopt rules that mitigate risks;
 1679 safeguard state agency digital assets, data, information, and
 1680 information technology resources to ensure availability,
 1681 confidentiality, and integrity; and support a security
 1682 governance framework. The department, acting through the Florida

Page 58 of 107

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

576-02447-25

20257026pb

1683 Digital Service, shall also:

1684 (b) ~~Develop, and annually update by February 1, a statewide~~
 1685 ~~cybersecurity strategic plan that includes security goals and~~
 1686 ~~objectives for cybersecurity, including the identification and~~
 1687 ~~mitigation of risk, proactive protections against threats,~~
 1688 ~~tactical risk detection, threat reporting, and response and~~
 1689 ~~recovery protocols for a cyber incident.~~

1690 ~~(c)~~ Develop and publish for use by state agencies a
 1691 cybersecurity governance framework that, at a minimum, includes
 1692 guidelines and processes for:

1693 1. ~~Establishing asset management procedures to ensure that~~
 1694 ~~an agency's information technology resources are identified and~~
 1695 ~~managed consistent with their relative importance to the~~
 1696 ~~agency's business objectives.~~

1697 2. ~~Using a standard risk assessment methodology that~~
 1698 ~~includes the identification of an agency's priorities,~~
 1699 ~~constraints, risk tolerances, and assumptions necessary to~~
 1700 ~~support operational risk decisions.~~

1701 3. ~~Completing comprehensive risk assessments and~~
 1702 ~~cybersecurity audits, which may be completed by a private sector~~
 1703 ~~vendor, and submitting completed assessments and audits to the~~
 1704 ~~department.~~

1705 4. ~~Identifying protection procedures to manage the~~
 1706 ~~protection of an agency's information, data, and information~~
 1707 ~~technology resources.~~

1708 5. ~~Establishing procedures for accessing information and~~
 1709 ~~data to ensure the confidentiality, integrity, and availability~~
 1710 ~~of such information and data.~~

1711 6. ~~Detecting threats through proactive monitoring of~~

Page 59 of 107

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

576-02447-25

20257026pb

1712 ~~events, continuous security monitoring, and defined detection~~
 1713 ~~processes.~~

1714 7. ~~Establishing agency cybersecurity incident response~~
 1715 ~~teams and describing their responsibilities for responding to~~
 1716 ~~cybersecurity incidents, including breaches of personal~~
 1717 ~~information containing confidential or exempt data.~~

1718 8. ~~Recovering information and data in response to a~~
 1719 ~~cybersecurity incident. The recovery may include recommended~~
 1720 ~~improvements to the agency processes, policies, or guidelines.~~

1721 9. Establishing a cybersecurity incident reporting process
 1722 that includes procedures for notifying the department and the
 1723 Department of Law Enforcement of cybersecurity incidents.

1724 a. The level of severity of the cybersecurity incident is
 1725 defined by the National Cyber Incident Response Plan of the
 1726 United States Department of Homeland Security as follows:

1727 (I) Level 5 is an emergency-level incident within the
 1728 specified jurisdiction that poses an imminent threat to the
 1729 provision of wide-scale critical infrastructure services;
 1730 national, state, or local government security; or the lives of
 1731 the country's, state's, or local government's residents.

1732 (II) Level 4 is a severe-level incident that is likely to
 1733 result in a significant impact in the affected jurisdiction to
 1734 public health or safety; national, state, or local security;
 1735 economic security; or civil liberties.

1736 (III) Level 3 is a high-level incident that is likely to
 1737 result in a demonstrable impact in the affected jurisdiction to
 1738 public health or safety; national, state, or local security;
 1739 economic security; civil liberties; or public confidence.

1740 (IV) Level 2 is a medium-level incident that may impact

Page 60 of 107

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

576-02447-25

20257026pb

1741 public health or safety; national, state, or local security;
1742 economic security; civil liberties; or public confidence.

1743 (V) Level 1 is a low-level incident that is unlikely to
1744 impact public health or safety; national, state, or local
1745 security; economic security; civil liberties; or public
1746 confidence.

1747 b. The cybersecurity incident reporting process must
1748 specify the information that must be reported by a state agency
1749 following a cybersecurity incident or ransomware incident,
1750 which, at a minimum, must include the following:

1751 (I) A summary of the facts surrounding the cybersecurity
1752 incident or ransomware incident.

1753 (II) The date on which the state agency most recently
1754 backed up its data; the physical location of the backup, if the
1755 backup was affected; and if the backup was created using cloud
1756 computing.

1757 (III) The types of data compromised by the cybersecurity
1758 incident or ransomware incident.

1759 (IV) The estimated fiscal impact of the cybersecurity
1760 incident or ransomware incident.

1761 (V) In the case of a ransomware incident, the details of
1762 the ransom demanded.

1763 c.(I) A state agency shall report all ransomware incidents
1764 and any cybersecurity incident determined by the state agency to
1765 be of severity level 3, 4, or 5 to the state chief information
1766 security officer ~~Cybersecurity Operations Center~~ and the
1767 Cybercrime Office of the Department of Law Enforcement as soon
1768 as possible but no later than 48 hours after discovery of the
1769 cybersecurity incident and no later than 12 hours after

Page 61 of 107

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

576-02447-25

20257026pb

1770 discovery of the ransomware incident. The report must contain
1771 the information required in sub-subparagraph b.

1772 (II) The state chief information security officer
1773 ~~Cybersecurity Operations Center~~ shall notify the President of
1774 the Senate and the Speaker of the House of Representatives of
1775 any severity level 3, 4, or 5 incident as soon as possible but
1776 no later than 12 hours after receiving a state agency's incident
1777 report. The notification must include a high-level description
1778 of the incident and the likely effects.

1779 d. A state agency shall report a cybersecurity incident
1780 determined by the state agency to be of severity level 1 or 2 to
1781 the state chief information security officer ~~Cybersecurity~~
1782 ~~Operations Center~~ and the Cybercrime Office of the Department of
1783 Law Enforcement as soon as possible, but no later than 96 hours
1784 after the discovery of the cybersecurity incident and no later
1785 than 72 hours after the discovery of the ransomware incident.

1786 The report must contain the information required in sub-
1787 subparagraph b.

1788 e. The state chief information security officer
1789 ~~Cybersecurity Operations Center~~ shall provide a consolidated
1790 incident report on a quarterly basis to the President of the
1791 Senate ~~and~~, the Speaker of the House of Representatives, ~~and the~~
1792 ~~Florida Cybersecurity Advisory Council. The report provided to~~
1793 ~~the Florida Cybersecurity Advisory Council may not contain the~~
1794 ~~name of any agency, network information, or system identifying~~
1795 ~~information but must contain sufficient relevant information to~~
1796 ~~allow the Florida Cybersecurity Advisory Council to fulfill its~~
1797 ~~responsibilities as required in s. 282.319(9).~~

1798 2.10- Incorporating information obtained through detection

Page 62 of 107

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

576-02447-25

20257026pb

1799 and response activities into the agency's cybersecurity incident
1800 response plans.

1801 ~~3.11-~~ Developing agency strategic and operational
1802 cybersecurity plans required pursuant to this section.

1803 ~~4.12-~~ Establishing the managerial, operational, and
1804 technical safeguards for protecting state government data and
1805 information technology resources that align with the state
1806 agency risk management strategy and that protect the
1807 confidentiality, integrity, and availability of information and
1808 data.

1809 ~~13. Establishing procedures for procuring information~~
1810 ~~technology commodities and services that require the commodity~~
1811 ~~or service to meet the National Institute of Standards and~~
1812 ~~Technology Cybersecurity Framework.~~

1813 ~~5.14-~~ Submitting after-action reports following a
1814 cybersecurity incident or ransomware incident. Such guidelines
1815 and processes for submitting after-action reports must be
1816 developed and published by December 1, 2022.

1817 ~~(f)(g)-~~ Annually provide cybersecurity training to all state
1818 agency technology professionals and employees with access to
1819 highly sensitive information which develops, assesses, and
1820 documents competencies by role and skill level. The
1821 cybersecurity training curriculum must include training on the
1822 identification of each cybersecurity incident severity level
1823 referenced in sub-subparagraph (b)1.a. ~~(c)9.a.~~ The training may
1824 be provided in collaboration with the Cybercrime Office of the
1825 Department of Law Enforcement, a private sector entity, or an
1826 institution of the State University System.

1827 ~~(h)- Operate and maintain a Cybersecurity Operations Center~~

Page 63 of 107

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

576-02447-25

20257026pb

1828 ~~led by the state chief information security officer, which must~~
1829 ~~be primarily virtual and staffed with tactical detection and~~
1830 ~~incident response personnel. The Cybersecurity Operations Center~~
1831 ~~shall serve as a clearinghouse for threat information and~~
1832 ~~coordinate with the Department of Law Enforcement to support~~
1833 ~~state agencies and their response to any confirmed or suspected~~
1834 ~~cybersecurity incident.~~

1835 ~~(i)- Lead an Emergency Support Function, ESF CYBER, under~~
1836 ~~the state comprehensive emergency management plan as described~~
1837 ~~in s. 252.35.~~

1838 (4) Each state agency head shall, at a minimum:

1839 (b) In consultation with the department, through the
1840 Florida Digital Service, and the Cybercrime Office of the
1841 Department of Law Enforcement, establish an agency cybersecurity
1842 response team to respond to a cybersecurity incident. The agency
1843 cybersecurity response team shall convene upon notification of a
1844 cybersecurity incident and must immediately report all confirmed
1845 or suspected incidents to the state chief information security
1846 officer, or his or her designee, and comply with all applicable
1847 guidelines and processes established pursuant to paragraph

1848 (3) (b) ~~(3) (e)~~.

1849 (c) Submit to the state chief information security officer
1850 ~~department~~ annually by July 31, the state agency's strategic and
1851 operational cybersecurity plans developed pursuant to rules and
1852 guidelines established by the state chief information security
1853 officer department, ~~through the Florida Digital Service.~~

1854 1. The state agency strategic cybersecurity plan must cover
1855 a 2-year ~~3-year~~ period and, at a minimum, define security goals,
1856 intermediate objectives, and projected agency costs for the

Page 64 of 107

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

576-02447-25

20257026pb

1857 strategic issues of agency information security policy, risk
 1858 management, security training, security incident response, and
 1859 disaster recovery. The plan must be based on the statewide
 1860 cybersecurity strategic plan created by the state chief
 1861 information security officer ~~department~~ and include performance
 1862 metrics that can be objectively measured to reflect the status
 1863 of the state agency's progress in meeting security goals and
 1864 objectives identified in the agency's strategic information
 1865 security plan.

1866 2. The state agency operational cybersecurity plan must
 1867 include a set of measures that objectively assesses the
 1868 performance of the agency's cybersecurity program in accordance
 1869 with its risk management plan progress report that objectively
 1870 measures progress made towards the prior operational
 1871 cybersecurity plan and a project plan that includes activities,
 1872 timelines, and deliverables for security objectives that the
 1873 state agency will implement during the current fiscal year.

1874 (d) Conduct, and update every 2 ~~3~~ years, a comprehensive
 1875 risk assessment, which may be completed by a private sector
 1876 vendor, to determine the security threats to the data,
 1877 information, and information technology resources, including
 1878 mobile devices and print environments, of the agency. The risk
 1879 assessment must comply with the risk assessment methodology
 1880 developed by the state chief information security officer
 1881 ~~department~~ and is confidential and exempt from s. 119.07(1),
 1882 except that such information shall be available to the Auditor
 1883 General, the state chief information security officer ~~Florida~~
 1884 ~~Digital Service~~ within the department, the Cybercrime Office of
 1885 the Department of Law Enforcement, and, for state agencies under

Page 65 of 107

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

576-02447-25

20257026pb

1886 the jurisdiction of the Governor, the Chief Inspector General.
 1887 If a private sector vendor is used to complete a comprehensive
 1888 risk assessment, it must attest to the validity of the risk
 1889 assessment findings. The comprehensive risk assessment must
 1890 include all of the following:

1891 1. The results of vulnerability and penetration tests on
 1892 any Internet website or mobile application that processes any
 1893 sensitive personal information or confidential information and a
 1894 plan to address any vulnerability identified in the tests.

1895 2. A written acknowledgment that the executive director or
 1896 the secretary of the agency, the chief financial officer of the
 1897 agency, and each executive manager as designated by the state
 1898 agency have been made aware of the risks revealed during the
 1899 preparation of the agency's operations cybersecurity plan and
 1900 the comprehensive risk assessment.

1901 (j) Develop a process for detecting, reporting, and
 1902 responding to threats, breaches, or cybersecurity incidents
 1903 which is consistent with the security rules, guidelines, and
 1904 processes established by the department through the Florida
 1905 Digital Service.

1906 1. All cybersecurity incidents and ransomware incidents
 1907 must be reported by state agencies. Such reports must comply
 1908 with the notification procedures and reporting timeframes
 1909 established pursuant to paragraph (3) (b) ~~(3) (e)~~.

1910 2. For cybersecurity breaches, state agencies shall provide
 1911 notice in accordance with s. 501.171.

1912 Section 19. Effective July 1, 2026, subsections (2), (3),
 1913 (4), (7), and (10) of section 282.318, Florida Statutes, as
 1914 amended by this act, are amended to read:

Page 66 of 107

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

576-02447-25

20257026pb

1915 282.318 Cybersecurity.-

1916 (2) As used in this section, the term "state agency" has
1917 the same meaning as provided in s. 282.0041, ~~except that the~~
1918 ~~term includes the Department of Legal Affairs, the Department of~~
1919 ~~Agriculture and Consumer Services, and the Department of~~
1920 ~~Financial Services.~~

1921 (3) ~~ASSET The department, acting through the Florida~~
1922 ~~Digital Service,~~ is the lead entity responsible for establishing
1923 enterprise technology and cybersecurity standards and processes
1924 for assessing state agency cybersecurity risks and determining
1925 appropriate security measures that comply with all national and
1926 state data compliance security standards. Such standards and
1927 processes must be consistent with generally accepted technology
1928 best practices, including the National Institute for Standards
1929 and Technology Cybersecurity Framework, for cybersecurity. ASSET
1930 ~~The department, acting through the Florida Digital Service,~~
1931 shall adopt rules that mitigate risks; safeguard state agency
1932 digital assets, data, information, and information technology
1933 resources to ensure availability, confidentiality, and
1934 integrity; and support a security governance framework. ASSET
1935 ~~The department, acting through the Florida Digital Service,~~
1936 shall also:

1937 (a) Designate an employee ~~of the Florida Digital Service~~ as
1938 the state chief information security officer. The state chief
1939 information security officer must have experience and expertise
1940 in security and risk management for communications and
1941 information technology resources. The state chief information
1942 security officer is responsible for the development of
1943 enterprise cybersecurity policy, standards, operation, and

Page 67 of 107

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

576-02447-25

20257026pb

1944 security architecture oversight ~~of cybersecurity~~ for state
1945 technology systems. The state chief information security officer
1946 shall be notified of all confirmed or suspected incidents or
1947 threats of state agency information technology resources and
1948 must report such incidents or threats to the state chief
1949 information officer ~~and the Governor.~~

1950 (b) Develop, and annually update by February 1, a statewide
1951 cybersecurity strategic plan that includes security goals and
1952 objectives for cybersecurity, including the identification and
1953 mitigation of risk, proactive protections against threats,
1954 tactical risk detection, threat reporting, and response and
1955 recovery protocols for a cyber incident.

1956 (c) ~~(b)~~ Develop and publish for use by state agencies a
1957 cybersecurity governance framework that, at a minimum, includes
1958 guidelines and processes for:

1959 1. Establishing asset management procedures to ensure that
1960 an agency's information technology resources are identified and
1961 managed consistently with their relative importance to the
1962 agency's business objectives.

1963 2. Using a standard risk assessment methodology that
1964 includes the identification of an agency's priorities,
1965 constraints, risk tolerances, and assumptions necessary to
1966 support operational risk decisions.

1967 3. Completing comprehensive risk assessments and
1968 cybersecurity audits, which may be completed by a private sector
1969 vendor, and submitting completed assessments and audits to the
1970 department.

1971 4. Identifying protection procedures to manage the
1972 protection of an agency's information, data, and information

Page 68 of 107

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

576-02447-25

20257026pb

1973 technology resources.

1974 5. Establishing procedures for accessing information and
 1975 data to ensure the confidentiality, integrity, and availability
 1976 of such information and data.

1977 6. Detecting threats through proactive monitoring of
 1978 events, continuous security monitoring, and defined detection
 1979 processes.

1980 7. Establishing agency cybersecurity incident response
 1981 teams and describing their responsibilities for responding to
 1982 cybersecurity incidents, including breaches of personal
 1983 information containing confidential or exempt data.

1984 8. Recovering information and data in response to a
 1985 cybersecurity incident. The recovery may include recommended
 1986 improvements to the agency processes, policies, or guidelines.

1987 9. Establishing a cybersecurity incident reporting process
 1988 that includes procedures for notifying ASSET ~~the department~~ and
 1989 the Department of Law Enforcement of cybersecurity incidents.

1990 a. The level of severity of the cybersecurity incident is
 1991 defined by the National Cyber Incident Response Plan of the
 1992 United States Department of Homeland Security as follows:

1993 (I) Level 5 is an emergency-level incident within the
 1994 specified jurisdiction that poses an imminent threat to the
 1995 provision of wide-scale critical infrastructure services;
 1996 national, state, or local government security; or the lives of
 1997 the country's, state's, or local government's residents.

1998 (II) Level 4 is a severe-level incident that is likely to
 1999 result in a significant impact in the affected jurisdiction to
 2000 public health or safety; national, state, or local security;
 2001 economic security; or civil liberties.

Page 69 of 107

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

576-02447-25

20257026pb

2002 (III) Level 3 is a high-level incident that is likely to
 2003 result in a demonstrable impact in the affected jurisdiction to
 2004 public health or safety; national, state, or local security;
 2005 economic security; civil liberties; or public confidence.

2006 (IV) Level 2 is a medium-level incident that may impact
 2007 public health or safety; national, state, or local security;
 2008 economic security; civil liberties; or public confidence.

2009 (V) Level 1 is a low-level incident that is unlikely to
 2010 impact public health or safety; national, state, or local
 2011 security; economic security; civil liberties; or public
 2012 confidence.

2013 b. The cybersecurity incident reporting process must
 2014 specify the information that must be reported by a state agency
 2015 following a cybersecurity incident or ransomware incident,
 2016 which, at a minimum, must include the following:

2017 (I) A summary of the facts surrounding the cybersecurity
 2018 incident or ransomware incident.

2019 (II) The date on which the state agency most recently
 2020 backed up its data; the physical location of the backup, if the
 2021 backup was affected; and if the backup was created using cloud
 2022 computing.

2023 (III) The types of data compromised by the cybersecurity
 2024 incident or ransomware incident.

2025 (IV) The estimated fiscal impact of the cybersecurity
 2026 incident or ransomware incident.

2027 (V) In the case of a ransomware incident, the details of
 2028 the ransom demanded.

2029 c.(I) A state agency shall report all ransomware incidents
 2030 and any cybersecurity incident determined by the state agency to

Page 70 of 107

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

576-02447-25

20257026pb

2031 be of severity level 3, 4, or 5 to the state chief information
 2032 security officer and the Cybercrime Office of the Department of
 2033 Law Enforcement as soon as possible but no later than 48 hours
 2034 after discovery of the cybersecurity incident and no later than
 2035 12 hours after discovery of the ransomware incident. The report
 2036 must contain the information required in sub-subparagraph b.

2037 (II) The state chief information security officer shall
 2038 notify the President of the Senate and the Speaker of the House
 2039 of Representatives of any severity level 3, 4, or 5 incident as
 2040 soon as possible but no later than 12 hours after receiving a
 2041 state agency's incident report. The notification must include a
 2042 high-level description of the incident and the likely effects.

2043 d. A state agency shall report a cybersecurity incident
 2044 determined by the state agency to be of severity level 1 or 2 to
 2045 the state chief information security officer and the Cybercrime
 2046 Office of the Department of Law Enforcement as soon as possible,
 2047 but no later than 96 hours after the discovery of the
 2048 cybersecurity incident and no later than 72 hours after the
 2049 discovery of the ransomware incident. The report must contain
 2050 the information required in sub-subparagraph b.

2051 e. The state chief information security officer shall
 2052 provide a consolidated incident report on a quarterly basis to
 2053 the Executive office of the Governor, the Commissioner of
 2054 Agriculture, the Chief Financial Officer, the Attorney General,
 2055 the President of the Senate, and the Speaker of the House of
 2056 Representatives.

2057 ~~10.2-~~ Incorporating information obtained through detection
 2058 and response activities into the agency's cybersecurity incident
 2059 response plans.

Page 71 of 107

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

576-02447-25

20257026pb

2060 ~~11.3-~~ Developing agency strategic and operational
 2061 cybersecurity plans required pursuant to this section.

2062 ~~12.4-~~ Establishing the managerial, operational, and
 2063 technical safeguards for protecting state government data and
 2064 information technology resources that align with the state
 2065 agency risk management strategy and that protect the
 2066 confidentiality, integrity, and availability of information and
 2067 data.

2068 13. In coordination with the state chief information
 2069 technology procurement officer, establishing procedures for
 2070 procuring information technology commodities and services that
 2071 require the commodity or service to meet the National Institute
 2072 of Standards and Technology Cybersecurity Framework.

2073 ~~14.5-~~ Submitting after-action reports following a
 2074 cybersecurity incident or ransomware incident. Such guidelines
 2075 and processes for submitting after-action reports must be
 2076 developed and published by July 1, 2027 ~~December 1, 2022~~.

2077 ~~(d)(e)~~ Assist state agencies in complying with this
 2078 section.

2079 ~~(e)(d)~~ In collaboration with the Cybercrime Office of the
 2080 Department of Law Enforcement and through the state chief
 2081 information security officer and the Division of Enterprise
 2082 Information Technology Workforce Development, annually provide
 2083 training for state agency information security managers and
 2084 computer security incident response team members that contains
 2085 training on cybersecurity, including cybersecurity threats,
 2086 trends, and best practices.

2087 ~~(f)(e)~~ Annually review the strategic and operational
 2088 cybersecurity plans of state agencies.

Page 72 of 107

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

576-02447-25

20257026pb

2089 ~~(g)(f)~~ Annually provide cybersecurity training through the
 2090 state chief information security officer and the Division of
 2091 Enterprise Information Technology Workforce Development to all
 2092 state agency technology professionals and employees with access
 2093 to highly sensitive information which develops, assesses, and
 2094 documents competencies by role and skill level. The
 2095 cybersecurity training curriculum must include training on the
 2096 identification of each cybersecurity incident severity level
 2097 referenced in sub-subparagraph (c)9.a. ~~(b)1-a-~~ The training may
 2098 be provided in collaboration with the Cybercrime Office of the
 2099 Department of Law Enforcement, a private sector entity, or an
 2100 institution of the State University System.

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

2102 (a) Designate an information security manager to administer
 2103 the cybersecurity program of the state agency. This designation
 2104 must be provided annually in writing to ASSET ~~the department~~ by
 2105 January 1. A state agency's information security manager, for
 2106 purposes of these information security duties, shall report
 2107 directly to the agency head.

2108 (b) In consultation with the state chief information
 2109 security officer ~~department, through the Florida Digital~~
 2110 ~~Service,~~ and the Cybercrime Office of the Department of Law
 2111 Enforcement, establish an agency cybersecurity response team to
 2112 respond to a cybersecurity incident. The agency cybersecurity
 2113 response team shall convene upon notification of a cybersecurity
 2114 incident and must immediately report all confirmed or suspected
 2115 incidents to the state chief information security officer, or
 2116 his or her designee, and comply with all applicable guidelines
 2117 and processes established pursuant to paragraph (3)(c) ~~(3)(b)~~.

Page 73 of 107

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

576-02447-25

20257026pb

2118 (c) Submit to state chief information security officer
 2119 annually by July 31 the state agency's strategic and operational
 2120 cybersecurity plans developed pursuant to rules and guidelines
 2121 established by the state chief information security officer.

2122 1. The state agency strategic cybersecurity plan must cover
 2123 a 2-year period and, at a minimum, define security goals,
 2124 intermediate objectives, and projected agency costs for the
 2125 strategic issues of agency information security policy, risk
 2126 management, security training, security incident response, and
 2127 disaster recovery. The plan must be based on the statewide
 2128 cybersecurity strategic plan created by the state chief
 2129 information security officer and include performance metrics
 2130 that can be objectively measured to reflect the status of the
 2131 state agency's progress in meeting security goals and objectives
 2132 identified in the agency's strategic information security plan.

2133 2. The state agency operational cybersecurity plan must
 2134 include a set of measures that objectively assess the
 2135 performance of the agency's cybersecurity program in accordance
 2136 with its risk management plan.

2137 (d) Conduct, and update every 2 years, a comprehensive risk
 2138 assessment, which may be completed by a private sector vendor,
 2139 to determine the security threats to the data, information, and
 2140 information technology resources, including mobile devices and
 2141 print environments, of the agency. The risk assessment must
 2142 comply with the risk assessment methodology developed by the
 2143 state chief information security officer and is confidential and
 2144 exempt from s. 119.07(1), except that such information shall be
 2145 available to the Auditor General, the state chief information
 2146 security officer, the Cybercrime Office of the Department of Law

Page 74 of 107

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

576-02447-25

20257026pb

2147 Enforcement, and, for state agencies under the jurisdiction of
 2148 the Governor, the Chief Inspector General. If a private sector
 2149 vendor is used to complete a comprehensive risk assessment, it
 2150 must attest to the validity of the risk assessment findings. The
 2151 comprehensive risk assessment must include all of the following:

2152 1. The results of vulnerability and penetration tests on
 2153 any Internet website or mobile application that processes any
 2154 sensitive personal information or confidential information and a
 2155 plan to address any vulnerability identified in the tests.

2156 2. A written acknowledgment that the executive director or
 2157 secretary of the agency, the chief financial officer of the
 2158 agency, and each executive manager as designated by the state
 2159 agency have been made aware of the risks revealed during the
 2160 preparation of the agency's operational cybersecurity plan and
 2161 the comprehensive risk assessment.

2162 (e) Develop, and periodically update, written internal
 2163 policies and procedures, which include procedures for reporting
 2164 cybersecurity incidents and breaches to the Cybercrime Office of
 2165 the Department of Law Enforcement and the state chief
 2166 information security officer ~~Florida Digital Service within the~~
 2167 ~~department~~. Such policies and procedures must be consistent with
 2168 the rules, guidelines, and processes established by ASSET ~~the~~
 2169 ~~department~~ to ensure the security of the data, information, and
 2170 information technology resources of the agency. The internal
 2171 policies and procedures that, if disclosed, could facilitate the
 2172 unauthorized modification, disclosure, or destruction of data or
 2173 information technology resources are confidential information
 2174 and exempt from s. 119.07(1), except that such information shall
 2175 be available to the Auditor General, the Cybercrime Office of

Page 75 of 107

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

576-02447-25

20257026pb

2176 the Department of Law Enforcement, the state chief information
 2177 security officer ~~the Florida Digital Service within the~~
 2178 ~~department~~, and, for state agencies under the jurisdiction of
 2179 the Governor, the Chief Inspector General.

2180 (f) Implement managerial, operational, and technical
 2181 safeguards and risk assessment remediation plans recommended by
 2182 ASSET ~~the department~~ to address identified risks to the data,
 2183 information, and information technology resources of the agency.
 2184 The state chief information security officer ~~department, through~~
 2185 ~~the Florida Digital Service~~, shall track implementation by state
 2186 agencies upon development of such remediation plans in
 2187 coordination with agency inspectors general.

2188 (g) Ensure that periodic internal audits and evaluations of
 2189 the agency's cybersecurity program for the data, information,
 2190 and information technology resources of the agency are
 2191 conducted. The results of such audits and evaluations are
 2192 confidential information and exempt from s. 119.07(1), except
 2193 that such information shall be available to the Auditor General,
 2194 the Cybercrime Office of the Department of Law Enforcement, the
 2195 state chief information security officer ~~Florida Digital Service~~
 2196 ~~within the department~~, and, for agencies under the jurisdiction
 2197 of the Governor, the Chief Inspector General.

2198 (h) Ensure that the cybersecurity requirements in the
 2199 written specifications for the solicitation, contracts, and
 2200 service-level agreement of information technology and
 2201 information technology resources and services meet or exceed the
 2202 applicable state and federal laws, regulations, and standards
 2203 for cybersecurity, including the National Institute of Standards
 2204 and Technology Cybersecurity Framework. Service-level agreements

Page 76 of 107

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

576-02447-25 20257026pb

2205 must identify service provider and state agency responsibilities
 2206 for privacy and security, protection of government data,
 2207 personnel background screening, and security deliverables with
 2208 associated frequencies.

2209 (i) Provide cybersecurity awareness training to all state
 2210 agency employees within 30 days after commencing employment, and
 2211 annually thereafter, concerning cybersecurity risks and the
 2212 responsibility of employees to comply with policies, standards,
 2213 guidelines, and operating procedures adopted by the state agency
 2214 to reduce those risks. The training may be provided in
 2215 collaboration with the Cybercrime Office of the Department of
 2216 Law Enforcement, a private sector entity, or an institution of
 2217 the State University System.

2218 (j) Develop a process for detecting, reporting, and
 2219 responding to threats, breaches, or cybersecurity incidents
 2220 which is consistent with the security rules, guidelines, and
 2221 processes established by ASSET ~~the department~~ through the state
 2222 chief information security officer ~~Florida Digital Service~~.

2223 1. All cybersecurity incidents and ransomware incidents
 2224 must be reported by state agencies. Such reports must comply
 2225 with the notification procedures and reporting timeframes
 2226 established pursuant to paragraph ~~(3) (c)~~ ~~(3) (b)~~.

2227 2. For cybersecurity breaches, state agencies shall provide
 2228 notice in accordance with s. 501.171.

2229 (k) Submit to the state chief information security officer
 2230 ~~Florida Digital Service~~, within 1 week after the remediation of
 2231 a cybersecurity incident or ransomware incident, an after-action
 2232 report that summarizes the incident, the incident's resolution,
 2233 and any insights gained as a result of the incident.

Page 77 of 107

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

576-02447-25 20257026pb

2234 (7) The portions of records made confidential and exempt in
 2235 subsections (5) and (6) shall be available to the Auditor
 2236 General, the Cybercrime Office of the Department of Law
 2237 Enforcement, the state chief information security officer, the
 2238 Legislature ~~Florida Digital Service~~ within the department, and,
 2239 for agencies under the jurisdiction of the Governor, the Chief
 2240 Inspector General. Such portions of records may be made
 2241 available to a local government, another state agency, or a
 2242 federal agency for cybersecurity purposes or in furtherance of
 2243 the state agency's official duties.

2244 (10) ASSET ~~The department~~ shall adopt rules relating to
 2245 cybersecurity and to administer this section.

2246 Section 20. Section 282.3185, Florida Statutes, is amended
 2247 to read:

2248 282.3185 Local government cybersecurity.—

2249 (1) SHORT TITLE.—This section may be cited as the "Local
 2250 Government Cybersecurity Act."

2251 (2) DEFINITION.—As used in this section, the term "local
 2252 government" means any county or municipality.

2253 (3) CYBERSECURITY TRAINING.—

2254 (a) The state chief information security officer ~~Florida~~
 2255 ~~Digital Service~~ shall:

2256 1. Develop a basic cybersecurity training curriculum for
 2257 local government employees. All local government employees with
 2258 access to the local government's network must complete the basic
 2259 cybersecurity training within 30 days after commencing
 2260 employment and annually thereafter.

2261 2. Develop an advanced cybersecurity training curriculum
 2262 for local governments which is consistent with the cybersecurity

Page 78 of 107

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

576-02447-25

20257026pb

2263 training required under s. 282.318(3)(f) ~~s. 282.318(3)(g)~~. All
 2264 local government technology professionals and employees with
 2265 access to highly sensitive information must complete the
 2266 advanced cybersecurity training within 30 days after commencing
 2267 employment and annually thereafter.

2268 (b) The state chief information security officer Florida
 2269 ~~Digital Service~~ may provide the cybersecurity training required
 2270 by this subsection in collaboration with the Cybercrime Office
 2271 of the Department of Law Enforcement, a private sector entity,
 2272 or an institution of the State University System.

2273 (4) CYBERSECURITY STANDARDS.—

2274 (a) Each local government shall adopt cybersecurity
 2275 standards that safeguard its data, information technology, and
 2276 information technology resources to ensure availability,
 2277 confidentiality, and integrity. The cybersecurity standards must
 2278 be consistent with generally accepted best practices for
 2279 cybersecurity, including the National Institute of Standards and
 2280 Technology Cybersecurity Framework.

2281 (b) Each county with a population of 75,000 or more must
 2282 adopt the cybersecurity standards required by this subsection by
 2283 January 1, 2024. Each county with a population of less than
 2284 75,000 must adopt the cybersecurity standards required by this
 2285 subsection by January 1, 2025.

2286 (c) Each municipality with a population of 25,000 or more
 2287 must adopt the cybersecurity standards required by this
 2288 subsection by January 1, 2024. Each municipality with a
 2289 population of less than 25,000 must adopt the cybersecurity
 2290 standards required by this subsection by January 1, 2025.

2291 (d) Each local government shall notify the state chief

Page 79 of 107

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

576-02447-25

20257026pb

2292 information security officer Florida Digital Service of its
 2293 compliance with this subsection as soon as possible.

2294 (5) INCIDENT NOTIFICATION.—

2295 (a) A local government shall provide notification of a
 2296 cybersecurity incident or ransomware incident to the state chief
 2297 information security officer Cybersecurity Operations Center,
 2298 the Cybercrime Office of the Department of Law Enforcement, and
 2299 the sheriff who has jurisdiction over the local government in
 2300 accordance with paragraph (b). The notification must include, at
 2301 a minimum, the following information:

2302 1. A summary of the facts surrounding the cybersecurity
 2303 incident or ransomware incident.

2304 2. The date on which the local government most recently
 2305 backed up its data; the physical location of the backup, if the
 2306 backup was affected; and if the backup was created using cloud
 2307 computing.

2308 3. The types of data compromised by the cybersecurity
 2309 incident or ransomware incident.

2310 4. The estimated fiscal impact of the cybersecurity
 2311 incident or ransomware incident.

2312 5. In the case of a ransomware incident, the details of the
 2313 ransom demanded.

2314 6. A statement requesting or declining assistance from ~~the~~
 2315 ~~Cybersecurity Operations Center~~, the Cybercrime Office of the
 2316 Department of Law Enforcement, or the sheriff who has
 2317 jurisdiction over the local government.

2318 (b)1. A local government shall report all ransomware
 2319 incidents and any cybersecurity incident determined by the local
 2320 government to be of severity level 3, 4, or 5 as provided in s.

Page 80 of 107

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

576-02447-25

20257026pb

2321 ~~282.318(3)(b) s. 282.318(3)(e)~~ to the state chief information
 2322 security officer ~~Cybersecurity Operations Center~~, the Cybercrime
 2323 Office of the Department of Law Enforcement, and the sheriff who
 2324 has jurisdiction over the local government as soon as possible
 2325 but no later than ~~12~~ 48 hours after discovery of the
 2326 cybersecurity incident and no later than ~~6~~ 12 hours after
 2327 discovery of the ransomware incident. The report must contain
 2328 the information required in paragraph (a).

2329 2. The state chief information security officer
 2330 ~~Cybersecurity Operations Center~~ shall notify the state chief
 2331 information officer, the Governor, the Commissioner of
 2332 Agriculture, the Chief Financial Officer, the Attorney General,
 2333 the President of the Senate, and the Speaker of the House of
 2334 Representatives of any severity level 3, 4, or 5 incident as
 2335 soon as possible but no later than 12 hours after receiving a
 2336 local government's incident report. The notification must
 2337 include a high-level description of the incident and the likely
 2338 effects.

2339 (c) A local government may report a cybersecurity incident
 2340 determined by the local government to be of severity level 1 or
 2341 2 as provided in s. 282.318(3)(b) ~~s. 282.318(3)(e)~~ to the state
 2342 chief information security officer ~~Cybersecurity Operations~~
 2343 ~~Center~~, the Cybercrime Office of the Department of Law
 2344 Enforcement, and the sheriff who has jurisdiction over the local
 2345 government. The report shall contain the information required in
 2346 paragraph (a).

2347 (d) The state chief information security officer
 2348 ~~Cybersecurity Operations Center~~ shall provide a consolidated
 2349 incident report by the 30th day after the end of each quarter ~~or~~

Page 81 of 107

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

576-02447-25

20257026pb

2350 ~~a quarterly basis~~ to the Governor, the Commissioner of
 2351 Agriculture, the Chief Financial Officer, the Attorney General,
 2352 the President of the Senate, and the Speaker of the House of
 2353 Representatives, ~~and the Florida Cybersecurity Advisory Council.~~
 2354 ~~The report provided to the Florida Cybersecurity Advisory~~
 2355 ~~Council may not contain the name of any local government,~~
 2356 ~~network information, or system identifying information but must~~
 2357 ~~contain sufficient relevant information to allow the Florida~~
 2358 ~~Cybersecurity Advisory Council to fulfill its responsibilities~~
 2359 ~~as required in s. 282.319(9).~~

2360 (6) AFTER-ACTION REPORT.—A local government must submit to
 2361 the state chief information security officer Florida Digital
 2362 ~~Service~~, within 1 week after the remediation of a cybersecurity
 2363 incident or ransomware incident, an after-action report that
 2364 summarizes the incident, the incident's resolution, and any
 2365 insights gained as a result of the incident. By December 1, 2027
 2366 ~~2022~~, the state chief information security officer Florida
 2367 ~~Digital Service~~ shall establish guidelines and processes for
 2368 submitting an after-action report.

2369 Section 21. Effective July 1, 2026, paragraph (a) of
 2370 subsection (3) and paragraphs (b) and (c) of subsection (5) of
 2371 section 282.3185, Florida Statutes, as amended by this act, are
 2372 amended to read:

2373 282.3185 Local government cybersecurity.—

2374 (3) CYBERSECURITY TRAINING.—

2375 (a) The state chief information security officer shall:

2376 1. Develop a basic cybersecurity training curriculum for
 2377 local government employees. All local government employees with
 2378 access to the local government's network must complete the basic

Page 82 of 107

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

576-02447-25

20257026pb

2379 cybersecurity training within 30 days after commencing
2380 employment and annually thereafter.

2381 2. Develop an advanced cybersecurity training curriculum
2382 for local governments which is consistent with the cybersecurity
2383 training required under s. 282.318(3)(g) ~~s. 282.318(3)(f)~~. All
2384 local government technology professionals and employees with
2385 access to highly sensitive information must complete the
2386 advanced cybersecurity training within 30 days after commencing
2387 employment and annually thereafter.

2388 (5) INCIDENT NOTIFICATION.—

2389 (b)1. A local government shall report all ransomware
2390 incidents and any cybersecurity incident determined by the local
2391 government to be of severity level 3, 4, or 5 as provided in s.
2392 282.318(3)(c) ~~s. 282.318(3)(b)~~ to the state chief information
2393 security officer, the Cybercrime Office of the Department of Law
2394 Enforcement, and the sheriff who has jurisdiction over the local
2395 government as soon as possible but no later than 12 hours after
2396 discovery of the cybersecurity incident and no later than 6
2397 hours after discovery of the ransomware incident. The report
2398 must contain the information required in paragraph (a).

2399 2. The state chief information security officer shall
2400 notify the state chief information officer, the Governor, the
2401 Commission of Agriculture, the Chief Financial Officer, the
2402 Attorney General, the President of the Senate and the Speaker of
2403 the House of Representatives of any severity level 3, 4, or 5
2404 incident as soon as possible but no later than 12 hours after
2405 receiving a local government's incident report. The notification
2406 must include a high-level description of the incident and the
2407 likely effects.

Page 83 of 107

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

576-02447-25

20257026pb

2408 (c) A local government may report a cybersecurity incident
2409 determined by the local government to be of severity level 1 or
2410 2 as provided in s. 282.318(3)(c) ~~s. 282.318(3)(b)~~ to the state
2411 chief information security officer, the Cybercrime Office of the
2412 Department of Law Enforcement, and the sheriff who has
2413 jurisdiction over the local government. The report shall contain
2414 the information required in paragraph (a).

2415 Section 22. Section 282.319, Florida Statutes, is repealed.

2416 Section 23. (1) POSITIONS.—

2417 (a) The following positions are established within the
2418 Agency for State Systems and Enterprise Technology:

2419 1. Chief operations officer.

2420 2. Chief information officer.

2421 (b) Effective July 1, 2026, the following positions are
2422 established within the Agency for State Systems and Enterprise
2423 Technology, all of whom shall be appointed by the executive
2424 director:

2425 1. Deputy executive director, who shall serve as the state
2426 chief information architect, and the following:

2427 a. A minimum of six lead technology coordinators. At least
2428 one coordinator shall be assigned to each of the following major
2429 program areas: health and human services, education, government
2430 operations, criminal and civil justice, agriculture and natural
2431 resources, and transportation and economic development.

2432 b. A minimum of six assistant technology coordinators. At
2433 least one coordinator shall be assigned to each of the following
2434 major program areas: health and human services, education,
2435 government operations, criminal and civil justice, agriculture
2436 and natural resources, and transportation and economic

Page 84 of 107

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

576-02447-25

20257026pb

2437 development.

2438 2. State chief information security officer and six lead
 2439 security consultants. One consultant shall be assigned to each
 2440 of the following major program areas: health and human services,
 2441 education, government operations, criminal and civil justice,
 2442 agriculture and natural resources, and transportation and
 2443 economic development.

2444 3. State chief data officer and the following:

2445 a. A minimum of three data specialists with at least one
 2446 specialist dedicated to each of the following areas of data
 2447 expertise:

2448 (I) Personally identifiable information.

2449 (II) Protected health information.

2450 (III) Criminal justice information services.

2451 b. A minimum of six data security consultants. At least one
 2452 consultant shall be assigned to each of the following major
 2453 program areas: health and human services, education, government
 2454 operations, criminal and civil justice, agriculture and natural
 2455 resources, and transportation and economic development.

2456 4. State chief information technology procurement officer
 2457 and a minimum of six lead information technology procurement
 2458 consultants. At least one coordinator shall be assigned to each
 2459 of the following major program areas: health and human services,
 2460 education, government operations, criminal and civil justice,
 2461 agriculture and natural resources, and transportation and
 2462 economic development.

2463 5. State chief technology officer and the following:

2464 a. A minimum of 42 information technology business analyst
 2465 consultants that shall be assigned to major program areas as

Page 85 of 107

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

576-02447-25

20257026pb

2466 follows:

2467 (I) At least 11 consultants shall be assigned to health and
 2468 human services and dedicated to state agencies at a minimum as
 2469 follows:

2470 (A) Two dedicated to the Department of Health.

2471 (B) Four dedicated to the Agency for Health Care

2472 Administration.

2473 (C) Three dedicated to the Department of Children and
 2474 Families.

2475 (D) Two dedicated to the remaining health and human
 2476 services state agencies.

2477 (II) At least four consultants shall be assigned to
 2478 education.

2479 (III) At least eight consultants shall be assigned to
 2480 government operations and dedicated to state agencies at a
 2481 minimum as follows:

2482 (A) Two dedicated to the Department of Financial Services.

2483 (B) One dedicated to the Department of Business and
 2484 Professional Regulation.

2485 (C) Two dedicated to the Department of Management Services.

2486 (D) Three dedicated to the remaining government operations
 2487 state agencies.

2488 (IV) At least six consultants shall be assigned to criminal
 2489 and civil justice and dedicated to state agencies at a minimum
 2490 as follows:

2491 (A) One dedicated to the Department of Law Enforcement.

2492 (B) Two dedicated to the Department of Corrections.

2493 (C) One dedicated to the Department of Juvenile Justice.

2494 (D) One dedicated to the Department of Legal Affairs.

Page 86 of 107

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

576-02447-25

20257026pb

2495 (E) One dedicated to the remaining criminal and civil
 2496 justice state agencies.

2497 (V) At least four consultants shall be assigned to
 2498 agriculture and natural resources and dedicated to state
 2499 agencies at a minimum as follows:

2500 (A) One dedicated the Department of Agriculture and
 2501 Consumer Services.

2502 (B) One dedicated to the Department of Environmental
 2503 Protection.

2504 (C) One dedicated to the Fish and Wildlife Conservation
 2505 Commission.

2506 (D) One dedicated to the remaining agriculture and natural
 2507 resources state agencies.

2508 (VI) At least nine consultants shall be assigned to
 2509 transportation and economic development and dedicated to state
 2510 agencies at a minimum as follows:

2511 (A) Two dedicated to the Department of Transportation.

2512 (B) Two dedicated to the Department of State.

2513 (C) One dedicated to the Department of Highway Safety and
 2514 Motor Vehicles.

2515 (D) Two dedicated to the Department of Commerce.

2516 (E) One dedicated to the Division of Emergency Management.

2517 (F) One dedicated to the remaining transportation and
 2518 economic development state agencies.

2519 b. A minimum of six information technology project
 2520 management professional consultants. At least one consultant
 2521 shall be assigned to each of the following major program areas:
 2522 health and human services, education, government operations,
 2523 criminal and civil justice, agriculture and natural resources,

Page 87 of 107

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

576-02447-25

20257026pb

2524 and transportation and economic development.

2525 c. A minimum of six information technology contract
 2526 management consultants. At least one consultant shall be
 2527 assigned to each of the following major program areas: health
 2528 and human services, education, government operations, criminal
 2529 and civil justice, agriculture and natural resources, and
 2530 transportation and economic development.

2531 d. A minimum of six information technology quality
 2532 assurance consultants. At least one consultant shall be assigned
 2533 to each of the following major program areas: health and human
 2534 services, education, government operations, criminal and civil
 2535 justice, agriculture and natural resources, and transportation
 2536 and economic development.

2537 (2) BUREAUS.—

2538 (a) The Division of Enterprise Information Technology
 2539 Services shall include:

2540 1. The Bureau of Enterprise Information Technology
 2541 Operations, responsible for assessing state agency information
 2542 technology needs and risks as established under s. 282.006,
 2543 Florida Statutes.

2544 2. The Bureau of Enterprise Information Technology Quality
 2545 Assurance, responsible for activities established under s.
 2546 282.006, Florida Statutes.

2547 3. The Bureau of Enterprise Information Technology Project
 2548 Management, responsible for project management oversight and
 2549 activities established under s. 282.006, Florida Statutes.

2550 4. The Bureau of Enterprise Information Technology Contract
 2551 Management, responsible for contract management oversight and
 2552 activities established under s. 282.006, Florida Statutes.

Page 88 of 107

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

576-02447-25

20257026pb

2553 (b) The Division of Enterprise Information Technology
 2554 Purchasing shall include:
 2555 1. The Bureau of Enterprise Information Technology
 2556 Procurement Services, responsible for procurement activities
 2557 established under s. 282.006, Florida Statutes.
 2558 2. The Bureau of Enterprise Information Technology
 2559 Procurement Policy and Oversight, responsible for activities
 2560 established under s. 282.006, Florida Statutes.
 2561 (3) WORKGROUP.—
 2562 (a) The chief information officer policy workgroup shall be
 2563 composed of all state agency chief information officers.
 2564 (b) The purpose of the workgroup is to provide the
 2565 Legislature with input and feedback regarding the structure,
 2566 budget, and governance of the Agency for State Systems and
 2567 Enterprise Technology.
 2568 (c) The chair of the workgroup shall be the interim state
 2569 chief information officer.
 2570 (d) The voting members of the workgroup shall include the
 2571 chair of the workgroup and the chief information officers from
 2572 the Department of Financial Services, the Department of
 2573 Agriculture and Consumer Services, and the Department of Legal
 2574 Affairs.
 2575 (e) The chair of the workgroup shall submit a report to the
 2576 Governor, the Commissioner of Agriculture, the Chief Financial
 2577 Officer, the Attorney General, the President of the Senate, and
 2578 the Speaker of the House of Representatives which includes
 2579 recommendations and justifications for changes by December 1,
 2580 2025. The final report must be voted on and accepted by a
 2581 unanimous vote of the voting members of the workgroup.

Page 89 of 107

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

576-02447-25

20257026pb

2582 (f) The workgroup shall expire after submission of the
 2583 report required in paragraph (e).
 2584 Section 24. Section 282.201, Florida Statutes, is amended
 2585 to read:
 2586 282.201 State data center.—The state data center is
 2587 established within the Northwest Regional Data Center pursuant
 2588 to s. 282.2011 the department. The provision of data center
 2589 services must comply with applicable state and federal laws,
 2590 regulations, and policies, including all applicable security,
 2591 privacy, and auditing requirements. The department shall appoint
 2592 a director of the state data center who has experience in
 2593 leading data center facilities and has expertise in cloud-
 2594 computing management.
 2595 ~~(1) STATE DATA CENTER DUTIES.—The state data center shall:~~
 2596 ~~(a) Offer, develop, and support the services and~~
 2597 ~~applications defined in service-level agreements executed with~~
 2598 ~~its customer entities.~~
 2599 ~~(b) Maintain performance of the state data center by~~
 2600 ~~ensuring proper data backup; data backup recovery; disaster~~
 2601 ~~recovery; and appropriate security, power, cooling, fire~~
 2602 ~~suppression, and capacity.~~
 2603 ~~(c) Develop and implement business continuity and disaster~~
 2604 ~~recovery plans, and annually conduct a live exercise of each~~
 2605 ~~plan.~~
 2606 ~~(d) Enter into a service-level agreement with each customer~~
 2607 ~~entity to provide the required type and level of service or~~
 2608 ~~services. If a customer entity fails to execute an agreement~~
 2609 ~~within 60 days after commencement of a service, the state data~~
 2610 ~~center may cease service. A service-level agreement may not have~~

Page 90 of 107

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

576-02447-25

20257026pb

2611 a term exceeding 3 years and at a minimum must:

2612 1. Identify the parties and their roles, duties, and

2613 responsibilities under the agreement.

2614 2. State the duration of the contract term and specify the

2615 conditions for renewal.

2616 3. Identify the scope of work.

2617 4. Identify the products or services to be delivered with

2618 sufficient specificity to permit an external financial or

2619 performance audit.

2620 5. Establish the services to be provided, the business

2621 standards that must be met for each service, the cost of each

2622 service by agency application, and the metrics and processes by

2623 which the business standards for each service are to be

2624 objectively measured and reported.

2625 6. Provide a timely billing methodology to recover the

2626 costs of services provided to the customer entity pursuant to s.

2627 215.422.

2628 7. Provide a procedure for modifying the service-level

2629 agreement based on changes in the type, level, and cost of a

2630 service.

2631 8. Include a right to audit clause to ensure that the

2632 parties to the agreement have access to records for audit

2633 purposes during the term of the service-level agreement.

2634 9. Provide that a service-level agreement may be terminated

2635 by either party for cause only after giving the other party and

2636 the department notice in writing of the cause for termination

2637 and an opportunity for the other party to resolve the identified

2638 cause within a reasonable period.

2639 10. Provide for mediation of disputes by the Division of

Page 91 of 107

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

576-02447-25

20257026pb

2640 Administrative Hearings pursuant to s. 120.573.

2641 (e) For purposes of chapter 273, be the custodian of

2642 resources and equipment located in and operated, supported, and

2643 managed by the state data center.

2644 (f) Assume administrative access rights to resources and

2645 equipment, including servers, network components, and other

2646 devices, consolidated into the state data center.

2647 1. Upon consolidation, a state agency shall relinquish

2648 administrative rights to consolidated resources and equipment.

2649 State agencies required to comply with federal and state

2650 criminal justice information security rules and policies shall

2651 retain administrative access rights sufficient to comply with

2652 the management control provisions of those rules and policies;

2653 however, the state data center shall have the appropriate type

2654 or level of rights to allow the center to comply with its duties

2655 pursuant to this section. The Department of Law Enforcement

2656 shall serve as the arbiter of disputes pertaining to the

2657 appropriate type and level of administrative access rights

2658 pertaining to the provision of management control in accordance

2659 with the federal criminal justice information guidelines.

2660 2. The state data center shall provide customer entities

2661 with access to applications, servers, network components, and

2662 other devices necessary for entities to perform business

2663 activities and functions, and as defined and documented in a

2664 service-level agreement.

2665 (g) In its procurement process, show preference for cloud-

2666 computing solutions that minimize or do not require the

2667 purchasing, financing, or leasing of state data center

2668 infrastructure, and that meet the needs of customer agencies,

Page 92 of 107

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

576-02447-25

20257026pb

2669 that ~~reduce costs, and that meet or exceed the applicable state~~
 2670 ~~and federal laws, regulations, and standards for cybersecurity.~~

2671 ~~(h) Assist customer entities in transitioning from state~~
 2672 ~~data center services to the Northwest Regional Data Center or~~
 2673 ~~other third party cloud computing services procured by a~~
 2674 ~~customer entity or by the Northwest Regional Data Center on~~
 2675 ~~behalf of a customer entity.~~

2676 (1)(2) USE OF THE STATE DATA CENTER.—

2677 ~~(a)~~ The following are exempt from the use of the state data
 2678 center: the Department of Law Enforcement, the Department of the
 2679 Lottery's Gaming System, Systems Design and Development in the
 2680 Office of Policy and Budget, the regional traffic management
 2681 centers as described in s. 335.14(2) and the Office of Toll
 2682 Operations of the Department of Transportation, the State Board
 2683 of Administration, state attorneys, public defenders, criminal
 2684 conflict and civil regional counsel, capital collateral regional
 2685 counsel, ~~and~~ the Florida Housing Finance Corporation, and the
 2686 Division of Emergency Management within the Executive Office of
 2687 the Governor.

2688 ~~(b) The Division of Emergency Management is exempt from the~~
 2689 ~~use of the state data center. This paragraph expires July 1,~~
 2690 ~~2025.~~

2691 (2)(3) AGENCY LIMITATIONS.—Unless exempt from the use of
 2692 the state data center pursuant to this section or authorized by
 2693 the Legislature, a state agency may not:

2694 (a) Create a new agency computing facility or data center,
 2695 or expand the capability to support additional computer
 2696 equipment in an existing agency computing facility or data
 2697 center; or

576-02447-25

20257026pb

2698 (b) Terminate services with the state data center without
 2699 giving written notice of intent to terminate services 180 days
 2700 before such termination.

2701 ~~(4) DEPARTMENT RESPONSIBILITIES.—The department shall~~
 2702 ~~provide operational management and oversight of the state data~~
 2703 ~~center, which includes:~~

2704 ~~(a) Implementing industry standards and best practices for~~
 2705 ~~the state data center's facilities, operations, maintenance,~~
 2706 ~~planning, and management processes.~~

2707 ~~(b) Developing and implementing cost-recovery mechanisms~~
 2708 ~~that recover the full direct and indirect cost of services~~
 2709 ~~through charges to applicable customer entities. Such cost-~~
 2710 ~~recovery mechanisms must comply with applicable state and~~
 2711 ~~federal regulations concerning distribution and use of funds and~~
 2712 ~~must ensure that, for any fiscal year, no service or customer~~
 2713 ~~entity subsidizes another service or customer entity. The~~
 2714 ~~department may recommend other payment mechanisms to the~~
 2715 ~~Executive Office of the Governor, the President of the Senate,~~
 2716 ~~and the Speaker of the House of Representatives. Such mechanisms~~
 2717 ~~may be implemented only if specifically authorized by the~~
 2718 ~~Legislature.~~

2719 ~~(c) Developing and implementing appropriate operating~~
 2720 ~~guidelines and procedures necessary for the state data center to~~
 2721 ~~perform its duties pursuant to subsection (1). The guidelines~~
 2722 ~~and procedures must comply with applicable state and federal~~
 2723 ~~laws, regulations, and policies and conform to generally~~
 2724 ~~accepted governmental accounting and auditing standards. The~~
 2725 ~~guidelines and procedures must include, but need not be limited~~
 2726 ~~to:~~

576-02447-25

20257026pb

2727 1. ~~Implementing a consolidated administrative support~~
 2728 ~~structure responsible for providing financial management,~~
 2729 ~~procurement, transactions involving real or personal property,~~
 2730 ~~human resources, and operational support.~~

2731 2. ~~Implementing an annual reconciliation process to ensure~~
 2732 ~~that each customer entity is paying for the full direct and~~
 2733 ~~indirect cost of each service as determined by the customer~~
 2734 ~~entity's use of each service.~~

2735 3. ~~Providing rebates that may be credited against future~~
 2736 ~~billings to customer entities when revenues exceed costs.~~

2737 4. ~~Requiring customer entities to validate that sufficient~~
 2738 ~~funds exist before implementation of a customer entity's request~~
 2739 ~~for a change in the type or level of service provided, if such~~
 2740 ~~change results in a net increase to the customer entity's cost~~
 2741 ~~for that fiscal year.~~

2742 5. ~~By November 15 of each year, providing to the Office of~~
 2743 ~~Policy and Budget in the Executive Office of the Governor and to~~
 2744 ~~the chairs of the legislative appropriations committees the~~
 2745 ~~projected costs of providing data center services for the~~
 2746 ~~following fiscal year.~~

2747 6. ~~Providing a plan for consideration by the Legislative~~
 2748 ~~Budget Commission if the cost of a service is increased for a~~
 2749 ~~reason other than a customer entity's request made pursuant to~~
 2750 ~~subparagraph 4. Such a plan is required only if the service cost~~
 2751 ~~increase results in a net increase to a customer entity for that~~
 2752 ~~fiscal year.~~

2753 7. ~~Standardizing and consolidating procurement and~~
 2754 ~~contracting practices.~~

2755 ~~(d) In collaboration with the Department of Law Enforcement~~

Page 95 of 107

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

576-02447-25

20257026pb

2756 and the Florida Digital Service, developing and implementing a
 2757 process for detecting, reporting, and responding to
 2758 cybersecurity incidents, breaches, and threats.

2759 ~~(c) Adopting rules relating to the operation of the state~~
 2760 ~~data center, including, but not limited to, budgeting and~~
 2761 ~~accounting procedures, cost-recovery methodologies, and~~
 2762 ~~operating procedures.~~

2763 ~~(5) NORTHWEST REGIONAL DATA CENTER CONTRACT. In order for~~
 2764 ~~the department to carry out its duties and responsibilities~~
 2765 ~~relating to the state data center, the secretary of the~~
 2766 ~~department shall contract by July 1, 2022, with the Northwest~~
 2767 ~~Regional Data Center pursuant to s. 287.057(11). The contract~~
 2768 ~~shall provide that the Northwest Regional Data Center will~~
 2769 ~~manage the operations of the state data center and provide data~~
 2770 ~~center services to state agencies.~~

2771 ~~(a) The department shall provide contract oversight,~~
 2772 ~~including, but not limited to, reviewing invoices provided by~~
 2773 ~~the Northwest Regional Data Center for services provided to~~
 2774 ~~state agency customers.~~

2775 ~~(b) The department shall approve or request updates to~~
 2776 ~~invoices within 10 business days after receipt. If the~~
 2777 ~~department does not respond to the Northwest Regional Data~~
 2778 ~~Center, the invoice will be approved by default. The Northwest~~
 2779 ~~Regional Data Center must submit approved invoices directly to~~
 2780 ~~state agency customers.~~

2781 Section 25. Section 1004.649, Florida Statutes, is
 2782 transferred, renumbered as section 282.0211, Florida Statutes,
 2783 and amended to read:
 2784 282.0211 ~~1004.649~~ Northwest Regional Data Center.-

Page 96 of 107

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

576-02447-25

20257026pb

2785 (1) For the purpose of providing data center services to
 2786 its state agency customers, the Northwest Regional Data Center
 2787 is designated as a state data center for all state agencies and
 2788 shall:

2789 (a) Operate under a governance structure that represents
 2790 its customers proportionally.

2791 (b) Maintain an appropriate cost-allocation methodology
 2792 that accurately bills state agency customers based solely on the
 2793 actual direct and indirect costs of the services provided to
 2794 state agency customers and ensures that, for any fiscal year,
 2795 state agency customers are not subsidizing other customers of
 2796 the data center. Such cost-allocation methodology must comply
 2797 with applicable state and federal regulations concerning the
 2798 distribution and use of state and federal funds.

2799 (c) Enter into a service-level agreement with each state
 2800 agency customer to provide services as defined and approved by
 2801 the governing board of the center. At a minimum, such service-
 2802 level agreements must:

2803 1. Identify the parties and their roles, duties, and
 2804 responsibilities under the agreement;

2805 2. State the duration of the agreement term, which may not
 2806 exceed 3 years, and specify the conditions for up to two
 2807 optional 1-year renewals of the agreement before execution of a
 2808 new agreement;

2809 3. Identify the scope of work;

2810 4. Establish the services to be provided, the business
 2811 standards that must be met for each service, the cost of each
 2812 service, and the process by which the business standards for
 2813 each service are to be objectively measured and reported;

576-02447-25

20257026pb

2814 5. Provide a timely billing methodology for recovering the
 2815 cost of services provided pursuant to s. 215.422;

2816 6. Provide a procedure for modifying the service-level
 2817 agreement to address any changes in projected costs of service;

2818 7. Include a right-to-audit clause to ensure that the
 2819 parties to the agreement have access to records for audit
 2820 purposes during the term of the service-level agreement;

2821 8. Identify the products or services to be delivered with
 2822 sufficient specificity to permit an external financial or
 2823 performance audit;

2824 9. Provide that the service-level agreement may be
 2825 terminated by either party for cause only after giving the other
 2826 party notice in writing of the cause for termination and an
 2827 opportunity for the other party to resolve the identified cause
 2828 within a reasonable period; and

2829 10. Provide state agency customer entities with access to
 2830 applications, servers, network components, and other devices
 2831 necessary for entities to perform business activities and
 2832 functions and as defined and documented in a service-level
 2833 agreement.

2834 (d) In its procurement process, show preference for cloud-
 2835 computing solutions that minimize or do not require the
 2836 purchasing or financing of state data center infrastructure,
 2837 that meet the needs of state agency customer entities, that
 2838 reduce costs, and that meet or exceed the applicable state and
 2839 federal laws, regulations, and standards for cybersecurity.

2840 (e) Assist state agency customer entities in transitioning
 2841 from state data center services to other third-party cloud-
 2842 computing services procured by a customer entity or by the

576-02447-25

20257026pb

2843 Northwest Regional Data Center on behalf of the customer entity.

2844 (f) Provide to the Board of Governors the total annual
2845 budget by major expenditure category, including, but not limited
2846 to, salaries, expenses, operating capital outlay, contracted
2847 services, or other personnel services by July 30 each fiscal
2848 year.

2849 (g) Provide to each state agency customer its projected
2850 annual cost for providing the agreed-upon data center services
2851 by September 1 each fiscal year.

2852 (h) By November 15 of each year, provide to the Office of
2853 Policy and Budget in the Executive Office of the Governor and to
2854 the chairs of the legislative appropriations committees the
2855 projected costs of providing data center services for the
2856 following fiscal year.

2857 (i) (h) Provide a plan for consideration by the Legislative
2858 Budget Commission if the governing body of the center approves
2859 the use of a billing rate schedule after the start of the fiscal
2860 year that increases any state agency customer's costs for that
2861 fiscal year.

2862 (j) (i) Provide data center services that comply with
2863 applicable state and federal laws, regulations, and policies,
2864 including all applicable security, privacy, and auditing
2865 requirements.

2866 (k) (j) Maintain performance of the data center facilities
2867 by ensuring proper data backup; data backup recovery; disaster
2868 recovery; and appropriate security, power, cooling, fire
2869 suppression, and capacity.

2870 (l) (k) ~~Prepare and submit state agency customer invoices to~~
2871 ~~the Department of Management Services for approval. Upon~~

Page 99 of 107

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

576-02447-25

20257026pb

2872 ~~approval or by default pursuant to s. 282.201(5),~~ Submit
2873 invoices to state agency customers.

2874 (m) (l) As funded in the General Appropriations Act, provide
2875 data center services to state agencies from multiple facilities.

2876 (2) Unless exempt from the requirement to use the state
2877 data center pursuant to s. 282.201(1) ~~s. 282.201(2)~~ or as
2878 authorized by the Legislature, a state agency may not do any of
2879 the following:

2880 (a) Terminate services with the Northwest Regional Data
2881 Center without giving written notice of intent to terminate
2882 services 180 days before such termination.

2883 (b) Procure third-party cloud-computing services without
2884 evaluating the cloud-computing services provided by the
2885 Northwest Regional Data Center.

2886 (c) Exceed 30 days from receipt of approved invoices to
2887 remit payment for state data center services provided by the
2888 Northwest Regional Data Center.

2889 (3) The Northwest Regional Data Center's authority to
2890 provide data center services to its state agency customers may
2891 be terminated if:

2892 (a) The center requests such termination to the Board of
2893 Governors, the President of the Senate, and the Speaker of the
2894 House of Representatives; or

2895 (b) The center fails to comply with the provisions of this
2896 section.

2897 (4) If such authority is terminated, the center has 1 year
2898 to provide for the transition of its state agency customers to a
2899 qualified alternative cloud-based data center that meets the
2900 enterprise architecture standards established by the Florida

Page 100 of 107

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

576-02447-25 20257026pb

2901 Digital Service.

2902 Section 26. Effective July 1, 2026, subsection (2) of

2903 section 20.22, Florida Statutes, is amended to read:

2904 20.22 Department of Management Services.—There is created a

2905 Department of Management Services.

2906 (2) The following divisions, programs, and services within

2907 the Department of Management Services are established:

2908 (a) Facilities Program.

2909 (b) ~~The Florida Digital Service.~~

2910 ~~(c)~~ Workforce Program.

2911 ~~(c) 1.~~ ~~(d) 1.~~ Support Program.

2912 2. Federal Property Assistance Program.

2913 ~~(d)~~ ~~(e)~~ Administration Program.

2914 ~~(e)~~ ~~(f)~~ Division of Administrative Hearings.

2915 ~~(f)~~ ~~(g)~~ Division of Retirement.

2916 ~~(g)~~ ~~(h)~~ Division of State Group Insurance.

2917 ~~(h)~~ ~~(i)~~ Division of Telecommunications.

2918 Section 27. Effective July 1, 2026, subsections (1), (5),

2919 (7), and (8) of section 282.802, Florida Statutes, are amended

2920 to read:

2921 282.802 Government Technology Modernization Council.—

2922 (1) The Government Technology Modernization Council, an

2923 advisory council as defined in s. 20.03(7), is located ~~created~~

2924 within ASSET ~~the department~~. Except as otherwise provided in

2925 this section, the advisory council shall operate in a manner

2926 consistent with s. 20.052.

2927 (5) The state chief information officer ~~Secretary of~~

2928 ~~Management Services~~, or his or her designee, shall serve as the

2929 ex officio, nonvoting executive director of the council.

Page 101 of 107

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

576-02447-25 20257026pb

2930 (7) ~~(a)~~ The council shall meet at least quarterly to:

2931 ~~(a) 1-~~ Recommend legislative and administrative actions that

2932 the Legislature and state agencies as defined in s. 282.0041 ~~or~~

2933 ~~282.318(2)~~ may take to promote the development of data

2934 modernization in this state.

2935 ~~(b) 2-~~ Assess and provide guidance on necessary legislative

2936 reforms and the creation of a state code of ethics for

2937 artificial intelligence systems in state government.

2938 ~~(c) 3-~~ Assess the effect of automated decision systems or

2939 identity management on constitutional and other legal rights,

2940 duties, and privileges of residents of this state.

2941 ~~(d) 4-~~ Evaluate common standards for artificial intelligence

2942 safety and security measures, including the benefits of

2943 requiring disclosure of the digital provenance for all images

2944 and audio created using generative artificial intelligence as a

2945 means of revealing the origin and edit of the image or audio, as

2946 well as the best methods for such disclosure.

2947 ~~(e) 5-~~ Assess the manner in which governmental entities and

2948 the private sector are using artificial intelligence with a

2949 focus on opportunity areas for deployments in systems across

2950 this state.

2951 ~~(f) 6-~~ Determine the manner in which artificial intelligence

2952 is being exploited by bad actors, including foreign countries of

2953 concern as defined in s. 287.138(1).

2954 ~~(g) 7-~~ Evaluate the need for curriculum to prepare school-

2955 age audiences with the digital media and visual literacy skills

2956 needed to navigate the digital information landscape.

2957 ~~(b) At least one quarterly meeting of the council must be a~~

2958 ~~joint meeting with the Florida Cybersecurity Advisory Council.~~

Page 102 of 107

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

576-02447-25

20257026pb

2959 (8) ~~By December 31, 2024, and~~ Each December 31 thereafter,
 2960 the council shall submit to the Governor, the Commissioner of
 2961 Agriculture, the Chief Financial Officer, the Attorney General,
 2962 the President of the Senate, and the Speaker of the House of
 2963 Representatives any legislative recommendations considered
 2964 necessary by the council to modernize government technology,
 2965 including:

(a) Recommendations for policies necessary to:

2967 1. Accelerate adoption of technologies that will increase
 2968 productivity of state enterprise information technology systems,
 2969 improve customer service levels of government, and reduce
 2970 administrative or operating costs.

2971 2. Promote the development and deployment of artificial
 2972 intelligence systems, financial technology, education
 2973 technology, or other enterprise management software in this
 2974 state.

2975 3. Protect Floridians from bad actors who use artificial
 2976 intelligence.

(b) Any other information the council considers relevant.

2978 Section 28. Effective July 1, 2026, section 282.604,
 2979 Florida Statutes, is amended to read:

2980 282.604 Adoption of rules.—~~ASSET~~ ~~The Department of~~
 2981 ~~Management Services~~ shall, with input from stakeholders, adopt
 2982 rules pursuant to ss. 120.536(1) and 120.54 for the development,
 2983 procurement, maintenance, and use of accessible electronic
 2984 information technology by governmental units.

2985 Section 29. Subsection (4) of section 287.0591, Florida
 2986 Statutes, is amended to read:

2987 287.0591 Information technology; vendor disqualification.—

Page 103 of 107

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

576-02447-25

20257026pb

2988 (4) If the department issues a competitive solicitation for
 2989 information technology commodities, consultant services, or
 2990 staff augmentation contractual services, the state chief
 2991 information officer must Florida Digital Service within the
 2992 ~~department shall~~ participate in such solicitations.

2993 Section 30. Subsection (4) of section 288.012, Florida
 2994 Statutes, is amended to read:

2995 288.012 State of Florida international offices; direct-
 2996 support organization.—The Legislature finds that the expansion
 2997 of international trade and tourism is vital to the overall
 2998 health and growth of the economy of this state. This expansion
 2999 is hampered by the lack of technical and business assistance,
 3000 financial assistance, and information services for businesses in
 3001 this state. The Legislature finds that these businesses could be
 3002 assisted by providing these services at State of Florida
 3003 international offices. The Legislature further finds that the
 3004 accessibility and provision of services at these offices can be
 3005 enhanced through cooperative agreements or strategic alliances
 3006 between private businesses and state, local, and international
 3007 governmental entities.

3008 (4) The Department of Commerce, in connection with the
 3009 establishment, operation, and management of any of its offices
 3010 located in another country, is exempt from the provisions of ss.
 3011 255.21, 255.25, and 255.254 relating to leasing of buildings;
 3012 ss. 283.33 and 283.35 relating to bids for printing; ss.
 3013 287.001-287.20 relating to purchasing and motor vehicles; and
 3014 ss. 282.0051 and 282.702-282.7101 ~~ss. 282.003-282.00515 and~~
 3015 ~~282.702-282.7101~~ relating to communications, and from all
 3016 statutory provisions relating to state employment.

Page 104 of 107

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

576-02447-25

20257026pb

3017 (a) The department may exercise such exemptions only upon
3018 prior approval of the Governor.

3019 (b) If approval for an exemption under this section is
3020 granted as an integral part of a plan of operation for a
3021 specified international office, such action shall constitute
3022 continuing authority for the department to exercise the
3023 exemption, but only in the context and upon the terms originally
3024 granted. Any modification of the approved plan of operation with
3025 respect to an exemption contained therein must be resubmitted to
3026 the Governor for his or her approval. An approval granted to
3027 exercise an exemption in any other context shall be restricted
3028 to the specific instance for which the exemption is to be
3029 exercised.

3030 (c) As used in this subsection, the term "plan of
3031 operation" means the plan developed pursuant to subsection (2).

3032 (d) Upon final action by the Governor with respect to a
3033 request to exercise the exemption authorized in this subsection,
3034 the department shall report such action, along with the original
3035 request and any modifications thereto, to the President of the
3036 Senate and the Speaker of the House of Representatives within 30
3037 days.

3038 Section 31. Effective July 1, 2026, paragraph (b) of
3039 subsection (4) of section 443.1113, Florida Statutes, is amended
3040 to read:

3041 443.1113 Reemployment Assistance Claims and Benefits
3042 Information System.—

3043 (4)

3044 (b) The department shall seek input on recommended
3045 enhancements from, at a minimum, the following entities:

Page 105 of 107

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

576-02447-25

20257026pb

3046 1. The Agency for State Systems and Enterprise Technology
3047 ~~Florida Digital Service within the Department of Management~~
3048 ~~Services.~~

3049 2. The General Tax Administration Program Office within the
3050 Department of Revenue.

3051 3. The Division of Accounting and Auditing within the
3052 Department of Financial Services.

3053 Section 32. Effective July 1, 2026, subsection (5) of
3054 section 943.0415, Florida Statutes, is amended to read:

3055 943.0415 Cybercrime Office.—There is created within the
3056 Department of Law Enforcement the Cybercrime Office. The office
3057 may:

3058 (5) Consult with the state chief information security
3059 officer of the Agency for State Systems and Enterprise
3060 Technology ~~Florida Digital Service within the Department of~~
3061 ~~Management Services~~ in the adoption of rules relating to the
3062 information technology security provisions in s. 282.318.

3063 Section 33. Effective July 1, 2026, subsection (3) of
3064 section 1004.444, Florida Statutes, is amended to read:

3065 1004.444 Florida Center for Cybersecurity.—

3066 (3) Upon receiving a request for assistance from a ~~the~~
3067 ~~Department of Management Services, the Florida Digital Service,~~
3068 ~~or another~~ state agency, the center is authorized, but may not
3069 be compelled by the agency, to conduct, consult on, or otherwise
3070 assist any state-funded initiatives related to:

3071 (a) Cybersecurity training, professional development, and
3072 education for state and local government employees, including
3073 school districts and the judicial branch; and

3074 (b) Increasing the cybersecurity effectiveness of the

Page 106 of 107

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

576-02447-25

20257026pb

3075 state's and local governments' technology platforms and
3076 infrastructure, including school districts and the judicial
3077 branch.

3078 Section 34. Except as otherwise provided in this act, this
3079 act shall take effect July 1, 2025.

APPEARANCE RECORD

Deliver both copies of this form to
Senate professional staff conducting the meeting

3/20/25

Meeting Date

SB 7026

Bill Number or Topic

Appropriation's

Committee

Amendment Barcode (if applicable)

Name Danny Jordan

Phone 850-264-6772

Address 3416 JONATHAN LANDING
Street

Email danny@team180.com

Tallahassee FL 32309
City State Zip

Speaking: For Against Information **OR** Waive Speaking: In Support Against

PLEASE CHECK ONE OF THE FOLLOWING:

I am appearing without compensation or sponsorship.

I am a registered lobbyist, representing:

Team 180

I am not a lobbyist, but received something of value for my appearance (travel, meals, lodging, etc.), sponsored by:

While it is a tradition to encourage public testimony, time may not permit all persons wishing to speak to be heard at this hearing. Those who do speak may be asked to limit their remarks so that as many persons as possible can be heard. If you have questions about registering to lobby please see Fla. Stat. §11.045 and Joint Rule 1. [2020-2022 Joint Rules.pdf flsenate.gov](#)

This form is part of the public record for this meeting.

The Florida Senate
BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Appropriations

BILL: SB 158

INTRODUCER: Senator Berman

SUBJECT: Coverage for Diagnostic and Supplemental Breast Examinations

DATE: March 19, 2025

REVISED: _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	<u>Davis</u>	<u>Betta</u>	<u>AEG</u>	Favorable
2.	<u>Davis</u>	<u>Sadberry</u>	<u>AP</u>	Favorable

I. Summary:

SB 158 prohibits the state group insurance program from imposing any cost-sharing liability for diagnostic breast examinations and supplemental breast examinations in any contract or plan for state employee health benefits that provides coverage for diagnostic breast examinations or supplemental breast examinations. The prohibition is effective January 1, 2026, consistent with the start of the new plan year.

The bill provides that if, under federal law, this prohibition would result in health savings account ineligibility under s. 223 of the Internal Revenue Code, the prohibition applies only to health savings account qualified high-deductible health plans with respect to the deductible of such a plan after the person has satisfied the minimum deductible under such plan.

The bill has a significant, negative fiscal impact on the state. See Section V., Fiscal Impact Statement.

The bill provides an effective date of January 1, 2026.

II. Present Situation:

Background

Rates of breast cancer vary among different groups of people. Rates vary between women and men and among people of different ethnicities and ages. Rates of breast cancer incidence (new cases) and mortality (death) are much lower among men than among women. The American Cancer Society made the following estimates regarding cancer among women in the U.S. during 2024:

- 310,720 new cases of invasive breast cancer (This includes new cases of primary breast cancer, but not breast cancer recurrences);
- 56,500 new cases of ductal carcinoma in situ (DCIS), a non-invasive breast cancer; and

- 42,250 breast cancer deaths.¹

The estimates for men in the U.S. for 2024 were:

- 2,790 new cases of invasive breast cancer (This includes new cases of primary breast cancers, but not breast cancer recurrences); and
- 530 breast cancer deaths.²

Breast cancer is the second most common form of cancer diagnosed in women, and it is estimated that one in eight women will be diagnosed with breast cancer in her lifetime.³ It accounts for 30 percent of all new female cancers in the United States each year.⁴ The median age at which a woman is diagnosed is 62 with a very small percentage of women who are diagnosed under the age of 45.⁵

Risks and Risk Factors

There are no absolute ways to prevent breast cancer as there might be with other forms of cancer; however, there are some risk factors that may increase a woman's chances of receiving a diagnosis. Some risk factors that are out of an individual's control are:

- Being born female;
- Aging beyond 55;
- Inheriting certain gene changes;
- Having a family or personal history of breast cancer;
- Being of certain race or ethnicity;
- Being taller;
- Having dense breast tissue;
- Having certain benign breast conditions;
- Starting menstrual periods early, usually before age 12;
- Having radiation to the chest; and
- Being exposed to the drug, diethylstilbestrol (DES).⁶

For many of the factors above, it is unclear why these characteristics make an individual more susceptible to a cancer diagnosis other than perhaps being female. However, men can and do receive breast cancer diagnoses, just in very small numbers. About one in every 100 breast cancers diagnosed in the United States is found in a man.⁷

¹ *Cancer Facts & Figures*, pgs. 10-11, American Cancer Society - [Cancer Facts & Figures 2024](#) (last visited February 20, 2025).

² *Id.*

³ American Cancer Society, *Key Statistics for Breast Cancer*, [Breast Cancer Statistics | How Common Is Breast Cancer? | American Cancer Society](#) (last visited February 25, 2025).

⁴ *Id.*

⁵ *Id.*

⁶ American Cancer Society, *Breast Cancer Risk Factors You Cannot Change*- [Breast Cancer Risk Factors You Can't Change | American Cancer Society](#) (last visited February 25, 2025).

⁷ Centers for Disease Control and Prevention, *Breast Cancer in Men*- [About Breast Cancer in Men | Breast Cancer | CDC](#) (last visited February 25, 2025).

Breast Cancer Screening

In Florida, a group, blanket, or franchise accident or health insurance policy issued, amended, delivered, or renewed in this state must provide coverage for at least the following:

- A baseline mammogram for any woman who is 35 years of age or older, but younger than 40 years of age.
- A mammogram every two years for any woman who is 40 years of age or older, but younger than 50 years of age, or more frequently based on the patient's physician's recommendation.
- A mammogram every year for any woman who is 50 years of age or older.
- One or more mammograms a year, based upon a physician's recommendation, for any woman who is at risk for breast cancer because of a personal or family history of breast cancer, because of having a history of biopsy-proven benign breast disease, because of having a mother, sister, or daughter who has or has had breast cancer, or because a woman has not given birth before the age of 30.⁸

Each such insurer must offer, for an appropriate additional premium, this same coverage without such coverage being subject to the deductible or coinsurance provisions of the policy.⁹

However, mammography is only the initial step in early detection and, by itself, unable to diagnose cancer. A mammogram is an x-ray of the breast.¹⁰ While screening mammograms are routinely performed to detect breast cancer in women who have no apparent symptoms, diagnostic mammograms are used after suspicious results on a screening mammogram or after some signs of breast cancer alert the physician to check the tissue.¹¹

If a mammogram shows something abnormal, early detection of breast cancer requires diagnostic follow-up or additional supplemental imaging required to rule out breast cancer or confirm the need for a biopsy.¹² An estimated 12-16 percent of women screened with modern digital mammography require follow-up imaging.¹³ Out-of-pocket costs are particularly burdensome on those who have previously been diagnosed with breast cancer, as diagnostic tests are recommended rather than traditional screening.¹⁴ When breast cancer is detected early, the five-year relative survival rate is ninety-nine percent.¹⁵

⁸ Section 627.6613(1), F.S.

⁹ Section 627.6613(3), F.S.

¹⁰ *What Is The Difference Between A Diagnostic Mammogram And A Screening Mammogram?* National Breast Cancer Foundation - <https://www.nationalbreastcancer.org/diagnostic-mammogram> (last visited February 25, 2025).

¹¹ *Id.*

¹² *Breast Cancer Screening & Early Detection*, Susan G. Komen Organization - <https://www.komen.org/breast-cancer/screening/> (last visited January 30, 2024).

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Early Detection*, National Breast Cancer Foundation - [Breast Cancer Early Detection - National Breast Cancer Foundation](https://www.nationalbreastcancer.org/early-detection/) (last visited February 25, 2025).

Regulation of Insurance in Florida

The Office of Insurance Regulation (OIR) regulates specified insurance products, insurers and other risk bearing entities in Florida.¹⁶ As part of their regulatory oversight, the OIR may suspend or revoke an insurer's certificate of authority under certain conditions.¹⁷ The OIR is responsible for examining the affairs, transactions, accounts, records, and assets of each insurer that holds a certificate of authority to transact insurance business in Florida.¹⁸ As part of the examination process, all persons being examined must make available to the OIR the accounts, records, documents, files, information, assets, and matters in their possession or control that relate to the subject of the examination.¹⁹ The OIR is also authorized to conduct market conduct examinations to determine compliance with applicable provisions of the Insurance Code.²⁰

The Agency for Health Care Administration (AHCA) regulates the quality of care by health maintenance organizations (HMO) under part III of ch. 641, F.S. Before receiving a certificate of authority from the OIR, an HMO must receive a Health Care Provider Certificate from AHCA.²¹ As part of the certificate process used by the agency, an HMO must provide information to demonstrate that the HMO has the ability to provide quality of care consistent with the prevailing standards of care.²²

State Employee Health Plan

For state employees who participate in the state employee benefit program, the Department of Management Services (DMS) through the Division of State Group Insurance (DSGI) administers the state group health insurance program (Program).²³ The Program is a cafeteria plan managed consistent with section 125 of the Internal Revenue Service Code.²⁴ To administer the program, DSGI contracts with third party administrators for self-insured plans, a fully insured HMO, and a pharmacy benefits manager for the state employees' self-insured prescription drug program, pursuant to s.110.12315, F.S. For the 2025 Plan Year, which began January 1, 2025, the HMO plans under contract with DSGI are Aetna, Capital Health Plan, and United Healthcare, and the preferred provider organization (PPO) plan is Florida Blue.²⁵

¹⁶ Section 20.121(3)(a), F.S. The Financial Services Commission, composed of the Governor, the Attorney General, the Chief Financial Officer, and the Commissioner of Agriculture, serves as a agency head of the Office of Insurance Regulation for purposes of rulemaking. Further, the Financial Services Commission appoints the commissioner of the Office of Insurance Regulation.

¹⁷ Section 624.418, F.S.

¹⁸ Section 624.316(1)(a), F.S.

¹⁹ Section 624.318(2), F.S.

²⁰ Section 624.3161, F.S.

²¹ Section 641.21(1), F.S.

²² Section 641.495, F.S.

²³ Section 110.123, F.S.

²⁴ A section 125 cafeteria plan is a type of employer offered, flexible health insurance plan that provides employees a menu of pre-tax and taxable qualified benefits to choose from, but employees must be offered at least one taxable benefit such as cash, and one qualified benefit, such as a Health Savings Account.

²⁵ Department of Management Services, Division of State Group Insurance, *2024 Open Enrollment Brochure for Active State Employee Participants*, available at https://www.mybenefits.myflorida.com/beta - open_enrollment (last visited February 25, 2025).

Breast Cancer Screening Coverage

Currently, the Program covers 100 percent of the costs of screening, preventive mammograms, (consistent with federal requirements related to essential health benefits coverage). Out of pocket costs, such as copayments, may vary for supplemental and diagnostic imaging based on the enrollee's plan and the provider selected.

III. Effect of Proposed Changes:

Section 1 amends s. 110.123, F.S., to provide definitions of "Cost-sharing requirement," "Diagnostic breast examination," and "Supplemental breast examination."

Section 2 amends s. 110.12303, F.S., to prohibit the state group insurance program from imposing any cost-sharing requirement on an enrollee (such as a deductible, copayment, coinsurance, or any other cost-sharing) with respect to coverage for diagnostic breast examinations and supplemental breast examinations in any contract or plan for state employee health benefits that provides coverage for diagnostic breast examinations or supplemental breast examinations. While current plans provide diagnostic breast examinations without cost sharing, cost sharing for supplemental examinations among the current plans vary. The bill provides parameters for what constitutes supplemental breast examinations, prohibiting cost sharing for examinations that are:

- Medically necessary and appropriate breast imaging examinations conducted in accordance with the most recent applicable guidelines of the National Comprehensive Cancer Network, which may include magnetic resonance imaging and ultrasounds and other types of examinations;
- Used when no abnormality is seen or suspected; and
- Based on personal or family medical history or other increased risk factors.

The bill provides that if, under federal law, this prohibition would result in health savings account ineligibility under s. 223 of the Internal Revenue Code, the prohibition applies only to health savings account qualified high-deductible health plans with respect to the deductible of such a plan after the person has satisfied the minimum deductible under such a plan.

Section 3 provides that the bill takes effect January 1, 2026.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None.

V. Fiscal Impact Statement:**A. Tax/Fee Issues:**

None.

B. Private Sector Impact:

The bill eliminates out-of-pocket costs for diagnostic and supplemental imaging for breast examinations, which is anticipated to improve access to these tests and likely to result in more patients receiving an earlier diagnosis. Early diagnosis increases the likelihood of successful treatment, which may result in savings for health insurers and HMOs.

C. Government Sector Impact:

The bill's prohibition on out-of-pocket costs for diagnostic and supplemental breast examinations has the potential to generate a higher insurance premium for the state group health plan. Historically, the state has covered premium inflation in the Program with General Revenue, rather than passing on premium increases to employees.

The Division of State Group Insurance within the Department of Management Services (DMS) estimates the bill will have an estimated fiscal impact of \$3.6 million annually in increased claim costs to state health plans due to the elimination of cost sharing and a projected increase in utilization.²⁶

The DMS included the following fiscal impact breakout between the PPO and HMO plans:

- Due to the differences in cost sharing arrangements, the PPO plan will experience a greater fiscal impact estimated at \$2.3 million. The removal of cost sharing as it relates to advanced imaging drives most of the estimated impact. The remaining impact is due to an estimated 13-27 percent increase in utilization for both the under age 45 population as well as the over age 45 population.
- HMO impacts are estimated to be lower due to the limited cost share responsibility of the standard HMO plan. Cumulative impacts for the HMO plans are estimated at approximately \$1.3 million (Self-Insured HMOs - \$1.31 million and Fully-Insured

²⁶ See Department of Management Services, *2025 Agency Legislative Bill Analysis for SB 158* at 3 (Feb. 24, 2025) (on file with the Senate Appropriations Committee on Agriculture, Environment, and General Government).

HMO - \$11,309). The removal of cost sharing as well as increased utilization drives the estimated impact.²⁷

The bill does not appear to implicate the Patient Protection and Affordable Care Act, as it is a cost-sharing bill only and does not mandate any new coverage or service or require any additions to the benchmark plan. Florida's EHB Benchmark Plan already includes diagnostic imaging.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 110.123 and 110.12303.

IX. Additional Information:

A. Committee Substitute – Statement of Changes:

(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.

This Senate Bill Analysis does not reflect the intent or official position of the bill's introducer or the Florida Senate.

²⁷ *Id.*

By Senator Berman

26-00164A-25

2025158__

1 A bill to be entitled
 2 An act relating to coverage for diagnostic and
 3 supplemental breast examinations; amending s. 110.123,
 4 F.S.; defining terms; amending s. 110.12303, F.S.;

5 prohibiting the state group insurance program from
 6 imposing any cost-sharing requirement upon an enrollee
 7 with respect to coverage for diagnostic breast
 8 examinations or supplemental breast examinations;
 9 providing applicability; providing an effective date.

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

11
 12 Section 1. Present paragraphs (a), (b) through (p), (q),
 13 and (r) of subsection (2) of section 110.123, Florida Statutes,
 14 are redesignated as paragraphs (b), (d) through (r), (t), and
 15 (u), respectively, new paragraphs (a) and (c) and paragraph (s)
 16 are added to that subsection, and paragraphs (c) and (d) of
 17 subsection (14) of that section are amended, to read:

18 110.123 State group insurance program.—

19 (2) DEFINITIONS.—As used in ss. 110.123-110.1239, the term:

20 (a) "Cost-sharing requirement" means an insured's
 21 deductible, coinsurance, copayment, or similar out-of-pocket
 22 expense.

23 (c) "Diagnostic breast examination" means a medically
 24 necessary and appropriate imaging examination of the breast, as
 25 determined in accordance with the most recent applicable
 26 guidelines of the National Comprehensive Cancer Network,
 27 including, but not limited to, an examination using diagnostic
 28 mammography, breast magnetic resonance imaging, or breast
 29

Page 1 of 3

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

26-00164A-25

2025158__

30 ultrasound, which is used to evaluate an abnormality that is
 31 seen or suspected during a screening examination for breast
 32 cancer.

33 (s) "Supplemental breast examination" means a medically
 34 necessary and appropriate imaging examination of the breast,
 35 conducted in accordance with the most recent applicable
 36 guidelines of the National Comprehensive Cancer Network,
 37 including, but not limited to, an examination using breast
 38 magnetic resonance imaging or breast ultrasound, which is:

39 1. Used to screen for breast cancer when there is no
 40 abnormality seen or suspected; and

41 2. Based on personal or family medical history or
 42 additional factors that may increase the person's risk of breast
 43 cancer.

44 (14) OTHER-PERSONAL-SERVICES EMPLOYEES (OPS).—

45 (c) The initial measurement period used to determine
 46 whether an employee hired before April 1, 2013, and paid from
 47 OPS funds is a full-time employee described in subparagraph
 48 (2)(g)1. ~~(2)(e)1-~~ is the 6-month period from April 1, 2013,
 49 through September 30, 2013.

50 (d) All other measurement periods used to determine whether
 51 an employee paid from OPS funds is a full-time employee
 52 described in paragraph (2)(g) ~~(2)(e)~~ must be for 12 consecutive
 53 months.

54 Section 2. Present subsections (5) and (6) of section
 55 110.12303, Florida Statutes, are redesignated as subsections (6)
 56 and (7), respectively, and a new subsection (5) is added to that
 57 section, to read:

58 110.12303 State group insurance program; additional

Page 2 of 3

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

26-00164A-25

2025158__

59 benefits; price transparency program; reporting.-
60 (5) In any contract or plan for state employee health
61 benefits which provides coverage for diagnostic breast
62 examinations or supplemental breast examinations, the state
63 group insurance program may not impose any cost-sharing
64 requirement upon an enrollee. If, under federal law, the
65 application of this subsection would result in health savings
66 account ineligibility under s. 223 of the Internal Revenue Code,
67 the prohibition under this subsection applies only to health
68 savings account qualified high-deductible health plans with
69 respect to the deductible of such a plan after the person has
70 satisfied the minimum deductible under s. 223 of the Internal
71 Revenue Code, except with respect to items or services that are
72 preventive care pursuant to s. 223(c)(2)(C) of the Internal
73 Revenue Code, in which case the requirements of s. 223(c)(2)(A)
74 of the Internal Revenue Code apply regardless of whether the
75 minimum deductible under s. 223 of the Internal Revenue Code has
76 been satisfied.
77 Section 3. This act shall take effect January 1, 2026.



The Florida Senate

Committee Agenda Request

To: Senator Ed Hooper, Chair
Committee on Appropriations

Subject: Committee Agenda Request

Date: March 7, 2025

I respectfully request that **Senate Bill #158**, relating to Coverage for Diagnostic and Supplemental Breast Examinations, be placed on the:

- committee agenda at your earliest possible convenience.
- next committee agenda.

A handwritten signature in black ink that reads "Lori Berman". The signature is written in a cursive style and is followed by a long horizontal line.

Senator Lori Berman
Florida Senate, District 26

3/20/2026

Meeting Date

The Florida Senate
APPEARANCE RECORD

SB 158

Bill Number or Topic

Appropriations

Committee

Deliver both copies of this form to
Senate professional staff conducting the meeting

Amendment Barcode (if applicable)

Name Georgia McKOWN

Phone 904 303 1611

Address 153 Deer Lake Circle

Email georgia@gamckown.com

Street

Ormond Beach, FL 32174

City

State

Zip

Speaking: For Against Information **OR** Waive Speaking: In Support Against

PLEASE CHECK ONE OF THE FOLLOWING:

I am appearing without compensation or sponsorship.

I am a registered lobbyist, representing:

American Cancer Society

I am not a lobbyist, but received something of value for my appearance (travel, meals, lodging, etc.), sponsored by:

While it is a tradition to encourage public testimony, time may not permit all persons wishing to speak to be heard at this hearing. Those who do speak may be asked to limit their remarks so that as many persons as possible can be heard. If you have questions about registering to lobby please see Fla. Stat. §11.045 and Joint Rule 1. [2020-2022JointRules.pdf \(flsenate.gov\)](#)

This form is part of the public record for this meeting.

S-001 (08/10/2021)

District Office
1380 Sarno Road
Suite C
Melbourne, FL 32935
(321) 409-2025

District Aide
Nancy Bernier
Bernier.Nancy@flsenate.gov

Legislative Aide
Tommy Unger
Unger.Thomas@flsenate.gov



Tallahassee Office:
302 SOB
404 South Monroe Street
Tallahassee, FL 32399-1300
(850) 487-5019
Fine.Randy@flsenate.gov

Legislative Aide
Anna Budko
Budko.Anna@flsenate.gov

Randy Fine
Florida Senate
Senator, District 19

March 20, 2025

The Honorable Ed Hooper
Chairman of Committee on Appropriations,
201 The Capitol
404 South Monroe Street
Tallahassee, FL 32399-1100

Dear Chairman Hooper,

I respectfully request an excused absence from the Committee on Appropriations meeting on March 20th, 2025.

Thank you in advance for your consideration of this request.

cc:
Chief of Staff Tim Sadberry
Deputy Chief of Staff John Shettle

Sincerely,

A handwritten signature in blue ink that reads "Randy A. Fine".

Randy Fine
State Senator, District 19

Governmental Oversight and Accountability, Chair
Community Affairs, Vice Chair
Joint Select Committee on Collective Bargaining, Alternating Chair
Appropriations -- Regulated Industries
Appropriations Committee on Agriculture, Environment, and General Government
Appropriations Committee on Pre-K - 12 Education -- Education Postsecondary
Brevard County Delegation

CourtSmart Tag Report

Room: SB 110
Caption: Senate Appropriations Committee

Case No.:

Type:
Judge:

Started: 3/20/2025 9:00:19 AM
Ends: 3/20/2025 10:11:42 AM Length: 01:11:24

9:00:19 AM	Sen. Hooper (Chair)
9:01:24 AM	S 158
9:01:38 AM	Sen. Berman
9:02:52 AM	Sen. Hooper
9:03:04 AM	Georgia McKeoynn, American Cancer Safety (waives in support)
9:03:09 AM	Sen. Polsky
9:04:14 AM	Sen. Hooper
9:04:36 AM	Sen. Harrell
9:05:18 AM	Sen. Hooper
9:05:52 AM	Sen. Sharief
9:05:53 AM	Sen. Hooper
9:05:57 AM	Sen. Berman
9:06:06 AM	Sen. Hooper
9:06:45 AM	S 7024
9:07:01 AM	Sen. Brodeur
9:07:18 AM	Sen. Hooper
9:08:12 AM	Sen. Sharief
9:08:22 AM	Sen. Brodeur
9:08:52 AM	Sen. Berman
9:09:34 AM	Sen. Hooper
9:10:32 AM	S 7026
9:10:41 AM	Sen. Harrell
9:28:01 AM	Sen. Hooper
9:28:30 AM	Sen. Grall
9:28:49 AM	Sen. Harrell
9:29:22 AM	Sen. Grall
9:29:54 AM	Sen. Harrell
9:30:38 AM	Sen. Grall
9:31:17 AM	Sen. Harrell
9:31:53 AM	Sen. Hooper
9:31:56 AM	Sen. Polsky
9:32:20 AM	Sen. Harrell
9:32:26 AM	Sen. Polsky
9:32:52 AM	Sen. Harrell
9:33:22 AM	Sen. Polsky
9:33:35 AM	Sen. Harrell
9:34:39 AM	Sen. Polsky
9:35:02 AM	Sen. Harrell
9:35:24 AM	Sen. Hooper
9:35:27 AM	Sen. Berman
9:36:17 AM	Sen. Harrell
9:37:23 AM	Sen. Berman
9:38:14 AM	Sen. Harrell
9:39:12 AM	Sen. Berman
9:39:39 AM	Sen. Harrell
9:40:39 AM	Sen. Hooper
9:40:43 AM	Sen. Pizzo
9:40:53 AM	Sen. Harrell
9:41:53 AM	Sen. Pizzo
9:42:34 AM	Sen. Harrell
9:43:13 AM	Sen. Pizzo
9:43:49 AM	Sen. Harrell

9:43:53 AM	Sen. Pizzo
9:43:56 AM	Sen. Harrell
9:44:01 AM	Sen. Hooper
9:44:14 AM	Am. 464614
9:44:20 AM	Sen. Harrell
9:45:13 AM	Sen. Hooper
9:45:21 AM	Sen. Pizzo
9:45:37 AM	Sen. Hooper
9:45:55 AM	Sen. Harrell
9:45:57 AM	Sen. Hooper
9:46:09 AM	Am. 208734
9:46:30 AM	Sen. Harrell
9:46:34 AM	Sen. Hooper
9:46:42 AM	Am. 784910
9:46:58 AM	Sen. Harrell
9:47:30 AM	Sen. Hooper
9:47:33 AM	Sen. Grall
9:47:48 AM	Sen. Harrell
9:48:21 AM	Sen. Hooper
9:48:23 AM	Sen. Pizzo
9:49:01 AM	Sen. Harrell
9:49:50 AM	Sen. Pizzo
9:50:25 AM	Sen. Harrell
9:50:56 AM	Sen. Hooper
9:51:03 AM	Am. 867736
9:51:22 AM	Sen. Harrell
9:52:23 AM	Sen. Hooper
9:53:04 AM	Sen. Rouson
9:53:24 AM	Danny Jordan, Team 180
9:56:58 AM	Sen. Pizzo
9:57:20 AM	D. Jordan
9:57:30 AM	Sen. Pizzo
9:57:53 AM	D. Jordan
9:57:57 AM	Sen. Pizzo
9:58:34 AM	D. Jordan
9:59:54 AM	Sen. Hooper
10:00:15 AM	Sen. Pizzo
10:01:46 AM	Sen. Hooper
10:01:48 AM	Sen. Polsky
10:02:18 AM	Sen. Harrell
10:03:44 AM	Sen. Hooper
10:03:46 AM	Sen. Collins
10:05:23 AM	Sen. Brodeur
10:06:49 AM	Sen. Hooper
10:07:40 AM	Sen. Harrell
10:09:30 AM	Sen. Hooper
10:10:47 AM	Sen. Pizzo
10:10:50 AM	Sen. Garcia
10:11:04 AM	Sen. Wright
10:11:10 AM	Sen. Trumbull
10:11:34 AM	Sen. Hooper