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:	SPB 7026
INTRODUCER:	For consideration by the Appropriations Committee
SUBJECT:	Information Technology
DATE:	March 19, 2025
REVISED:	

ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
Hunter/Davis	Sadberry		**Pre-meeting**

I. Summary:

SPB 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, and requires the Northwest Regional Data Center (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 cyberattacks[2] 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 malware[5] 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 Services[12] 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 agency[18] 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 agencies[23] to meet certain requirements to enhance the cybersecurity[24] 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 Council[32] (CAC) within the DMS[33] 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] [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.

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 Northwest Regional Data Center, 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 Model[51] 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 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.

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 Security Officer, Chief Data 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.

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 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 transfers s. 1004.649, F.S., regarding the state data center services provided by the Northwest Regional Data Center (NWRDC), to s. 282.211, F.S., 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 abolishes the FLDS within the DMS in s. 20.22, F.S., effective July 1, 2026.

Section 27 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 28 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 29 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 30 makes technical, conforming changes to cross-references in s. 288.012, F.S.

Section 31 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 32 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 33 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 34 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 $3,481,212 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, 282.0211, 282.201, 282.318, 282.3185, 282.802, 282.604, 287.0591, 288.012, 443.1113, 943.0415, and 1004.444.

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

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

The bill transfers section 1004.649 of the Florida Statutes to section 282.0211 of the Florida Statutes.

IX. Additional Information:

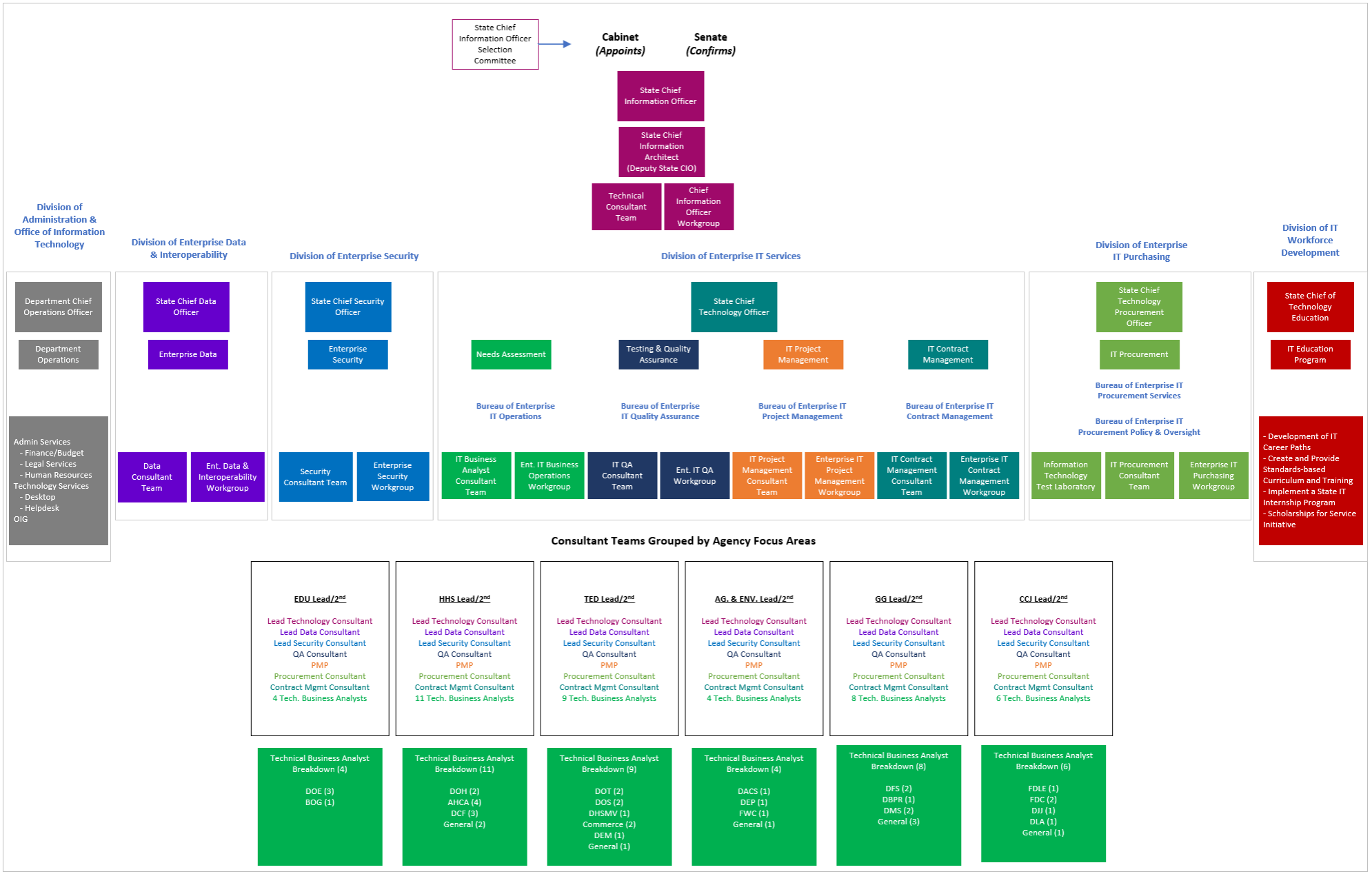
A. Committee Substitute – Statement of Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.

Exhibit 1


State Chief Information Officer Selection Committee
Cabinet (Appoints)
Senate (Confirms)
State Chief Information Officer
State Chief Information Architect (Deputy State CIO)
Technical Consultant Team
Chief Information Officer Workgroup
Division of Administration & Office of Information Technology
Division of Enterprise Data & Interoperability
Division of Enterprise Security
Division of Enterprise IT Services
Division of Enterprise IT Purchasing
Division of IT Workforce Development
Department Chief Operations Officer
Department Operations
Admin Services
- Finance/Budget
- Legal Services
- Human Resources
Technology Services
- Desktop
- Helpdesk
OIG
State Chief Data Officer
Enterprise Data
Data Consultant Team
Ent. Data & Interoperability Workgroup
State Chief Security Officer
Enterprise Security
Security Consultant Team
Enterprise Security Workgroup
State Chief Technology Officer
Needs Assessment
Testing & Quality Assurance
IT Project Management
IT Contract Management
Bureau of Enterprise IT Operations
Bureau of Enterprise IT Quality Assurance
Bureau of Enterprise IT Project Management
Bureau of Enterprise IT Contract Management
IT Business Analyst Consultant Team
Ent. IT Business Operations Workgroup
IT QA Consultant Team
Ent. IT QA Workgroup
IT Project Management Consultant Team
Enterprise IT Project Management Workgroup
IT Contract Management Consultant Team
Enterprise IT Contract Management Workgroup
State Chief Technology Procurement Officer
IT Procurement
Bureau of Enterprise IT Procurement Services
Bureau of Enterprise IT Procurement Policy & Oversight
Information Technology Test Laboratory
IT Procurement Consultant Team
Enterprise IT Purchasing Workgroup
State Chief of Technology Education
IT Education Program
- Development of IT Career Paths
- Create and Provide Standards-based Curriculum and Training
- Implement a State IT Internship Program
- Scholarships for Service Initiative
Consultant Teams Grouped by Agency Focus Areas
EDU Lead/2nd
Lead Technology Consultant
Lead Data Consultant
Lead Security Consultant
QA Consultant
PMP
Procurement Consultant
Contract Mgmt Consultant
4 Tech. Business Analysts
HHS Lead/2nd
Lead Technology Consultant
Lead Data Consultant
Lead Security Consultant
QA Consultant
PMP
Procurement Consultant
Contract Mgmt Consultant
11 Tech. Business Analysts
TED Lead/2nd
Lead Technology Consultant
Lead Data Consultant
Lead Security Consultant
QA Consultant
PMP
Procurement Consultant
Contract Mgmt Consultant
9 Tech. Business Analysts
AG. & ENV. Lead/2nd
Lead Technology Consultant
Lead Data Consultant
Lead Security Consultant
QA Consultant
PMP
Procurement Consultant
Contract Mgmt Consultant
4 Tech. Business Analysts
GG Lead/2nd
Lead Technology Consultant
Lead Data Consultant
Lead Security Consultant
QA Consultant
PMP
Procurement Consultant
Contract Mgmt Consultant
8 Tech. Business Analysts
CCJ Lead/2nd
Lead Technology Consultant
Lead Data Consultant
Lead Security Consultant
QA Consultant
PMP
Procurement Consultant
Contract Mgmt Consultant
6 Tech. Business Analysts
Technical Business Analyst Breakdown (4)
DOE (3)
BOG (1)
Technical Business Analyst Breakdown (11)
DOH (2)
AHCA (4)
DCF (3)
General (2)
Technical Business Analyst Breakdown (9)
DOT (2)
DOS (2)
DHSMV (1)
Commerce (2)
DEM (1)
General (1)
Technical Business Analyst Breakdown (4)
DACS (1)
DEP (1)
FWC (1)
General (1)
Technical Business Analyst Breakdown (8)
DFS (2)
DBPR (1)
DMS (2)
General (3)
Technical Business Analyst Breakdown (6)
FDLE (1)
FDC (2)
DJJ (1)
DLA (1)
General (1)