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:	CS/SB 480
INTRODUCER:	Appropriations Committee; Appropriations Committee on Agriculture, Environment, and General Government; and Senator Harrell
SUBJECT:	Information Technology
DATE:	February 16, 2026 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Hunter	Betta	AEG	**Fav/CS**
2.	Hunter	Sadberry	AP	**Fav/CS**

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/CS/SB 480 establishes the Division of Integrated Government Innovation and Technology (DIGIT) under the Executive Office of the Governor. The Florida Digital Service (FLDS) is transferred to DIGIT via a Type 2 transfer. The state Chief Information Officer (CIO) will serve as the DIGIT's executive director, appointed by the Governor and confirmed by the Senate.

The DIGIT will absorb non-operational functions of the FLDS, adding responsibilities such as master data management, legacy system needs assessments, and information technology (IT) expenditure tracking. The DIGIT will also develop career training programs for the state's IT workforce.

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 It eliminates the Cybersecurity Advisory Council, removes outdated data center management language from law, requires the Northwest Regional Data Center (NWRDC) to meet or exceed the standards established by the DIGIT, and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 no fiscal impact on state expenditures. See Section V., Fiscal Impact Statement.

The bill takes effect January 5, 2027.

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 was 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.

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]

---

[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 January 22, 2026).
[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. Infosecurity Magazine, *US the Primary Target of "Significant" Cyber-Attacks*, https://www.infosecurity-magazine.com/news/us-primary-target-significant/#:~:text=The%20US%20experienced%20far%20more,)%20and%20Vietnam%20(6). (last visited January 22, 2026).
[3] *Id.*
[4] S&P Global, *Pipeline operators must start reporting cyberattacks to government: TSA orders*, https://www.spglobal.com/energy/en/news-research/latest-news/electric-power/052721-pipeline-operators-must-start-reporting-cyberattacks-to-government-tsa-orders (last visited January 22, 2026).
[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 January 22, 2026).
[6] Cybersecurity and Infrastructure Agency, *Ransomware 101,* https://www.cisa.gov/stopransomware/ransomware-101 (last visited January 22, 2026).
[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 January 22, 2026).

Information Technology and Cybersecurity Management

The Department of Management Services (DMS) oversees 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 IT 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 and publish 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
- 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.

---

[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.
[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

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;
- 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;

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.

[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.

- 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 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
- Develop a process 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

[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*, Fortra (Dec. 1, 2020), https://www.digitalguardian.com/blog/what-nist-compliance (last visited January 22, 2026).
[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.

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;
- 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

[35] Section 282.319(3), F.S.
[36] Section 282.319(9), F.S.
[37] Section 282.319(10), F.S.
[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 January 22, 2026).

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]

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]

---

[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 January 22, 2026).
[41] *Id.*
[42] Section 282.318(3)(c)9.a, F.S.
[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.

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.

Inspector General

The Office of Chief Inspector General (CIG) is responsible for promoting accountability, integrity, and efficiency in agencies under the Governor's jurisdiction.[51] The CIG is required to do the following:

- Initiate, supervise, and coordinate investigations; recommend policies; and carry out other activities designed to deter, detect, prevent, and eradicate fraud, waste, abuse, mismanagement, and misconduct in government;
- Investigate, upon receipt of a complaint or for cause, any administrative action of any agency, the administration of which is under the direct supervision of the Governor;
- Request such assistance and information as may be necessary for the performance of the CIG's duties;
- Examine the records and reports of any agency the administration of which is under the direct supervision of the Governor;
- Coordinate complaint-handling activities with agencies;
- Coordinate the activities of the Whistle-blower's Act and maintain the whistle-blower's hotline to receive complaints and information concerning the possible violation of law or

[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.
[51] Section 14.32(1), F.S.

administrative rules, mismanagement, fraud, waste, abuse of authority, malfeasance, or a substantial or specific danger to the health, welfare, or safety of the public;
- Report expeditiously to and cooperate fully with the Department of Law Enforcement, the Department of Legal Affairs, and other law enforcement agencies when there are recognizable grounds to believe that there has been a violation of criminal law or that a civil action should be initiated;
- Act as liaison with outside agencies and the federal government to promote accountability, integrity, and efficiency in state government;
- Act as liaison and monitor the activities of the inspectors general in the agencies under the Governor's jurisdiction;
- Review, evaluate, and monitor the policies, practices, and operations of the Executive Office of the Governor; and
- Conduct special investigations and management reviews at the request of the Governor.[52]

Authorized under s. 20.055, F.S., an Office of Inspector General (OIG) is established in each state agency[53] to provide a central point for the coordination of and responsibility for activities that promote accountability, integrity, and efficiency in government.[54] Each agency OIG is responsible for the following:
- Advising in the development of performance measures, standards, and procedures for the evaluation of state agency programs;
- Assessing the reliability and validity of information provided by the agency on performance measures and standards, and making recommendations for improvement, if necessary;
- Reviewing the actions taken by the agency to improve program performance and meet program standards, and making recommendations for improvement, if necessary;
- Supervising and coordinating audits, investigations, and management reviews relating to the programs and operations of the agency;
- Conducting, supervising, or coordinating other activities carried out or financed by the agency for the purpose of promoting economy and efficiency in the administration of, or preventing and detecting fraud and abuse in, its programs and operations;
- Keeping the agency head,[55] or the CIG for agencies under the jurisdiction of the Governor, informed concerning fraud, abuses, and deficiencies relating to programs and operations administered or financed by the agency; recommending corrective action concerning fraud, abuses, and deficiencies; and reporting on the progress made in implementing corrective action;

[52] Section 14.32(2), F.S.
[53] Section 20.055(1)(d), F.S. defines the term "state agency" as each department created pursuant to ch. 20, F.S., and the Executive Office of the Governor, the Department of Military Affairs, the Fish and Wildlife Conservation Commission, the Office of Insurance Regulation of the Financial Services Commission, the Office of Financial Regulation of the Financial Services Commission, the Public Service Commission, the Board of Governors of the State University System, the Florida Housing Finance Corporation, the Florida Gaming Control Commission, and the state courts system.
[54] Section 20.055(2), F.S.
[55] Section 20.055(1)(a), F.S., defines the term "agency head" as the Governor, a Cabinet officer, a secretary as defined in s. 20.03(5), F.S., or an executive director as defined in s. 20.03(6), F.S., the chair of the Public Service Commission, the Director of the Office of Insurance Regulation of the Financial Services Commission, the Director of the Office of Financial Regulation of the Financial Services Commission, the board of directors of the Florida Housing Finance Corporation, the chair of the Florida Gaming Control Commission, and the Chief Justice of the State Supreme Court.

- Ensuring effective coordination and cooperation between the Auditor General, federal auditors, and other governmental bodies to avoid duplication;
- Reviewing rules relating to the programs and operations of the agency and making recommendations concerning their impact;
- Ensuring that an appropriate balance is maintained between audit, investigative, and other accountability activities; and
- Complying with the General Principles and Standards for Offices of Inspector General as published and revised by the Association of Inspectors General.[56]

III. Effect of Proposed Changes:

Section 1 provides for a Type Two transfer pursuant to s. 20.06, F.S., of all duties, functions, records, pending issues, existing contracts, administrative authority, and administrative rules from the Florida Digital Service (FLDS) to the Division of Integrated Government Innovation and Technology (DIGIT). Any unexpended balances of public funds will revert or will be appropriated or allocated as provided in the General Appropriations Act or otherwise by law.

Section 2 creates s. 14.205, F.S., to create the DIGIT to serve as Florida's centralized Information Technology (IT) governance body, overseeing statewide technology initiatives and cybersecurity efforts. The DIGIT will be led by the Governor.

The Executive Director of the DIGIT serves as the State Chief Information Officer (CIO). The Governor must appoint a CIO subject to confirmation by the Senate. 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 IT 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 IT regulations, digital services, and cybersecurity compliance frameworks.

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

[56] Section 20.055(2), F.S.

- 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 IT trends;
- IT governance and policy development by demonstrating an understanding of statewide IT governance structures, digital services, and IT procurement policies; and
- Public sector IT management by demonstrating familiarity with government IT funding models, procurement requirements, and legislative processes affecting IT 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 IT 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.

The deputy director of the DIGIT will serve as the deputy chief information officer. The CIO will also select a state chief information security officer, a state chief data officer, a state chief technology officer, and a state chief technology procurement officer.

Section 3 provides that, until a permanent CIO is appointed, the current CIO of the Department of Management Services (DMS) must be transferred to the DIGIT and serve as the interim CIO, assuming all responsibilities of the Executive Director of the DIGIT. To establish long-term leadership, the Governor must appoint a permanent CIO by June 30, 2027.

Section 4 amends s. 20.055, F.S., by requiring each inspector general to review and evaluate his or her agency's compliance with IT reporting requirements and standards for IT projects, contracts, and procurements published by the DIGIT and provide an annual agency IT compliance report to the agency head, the Auditor General, and if applicable, the Chief Inspector General (CIG) by September 30 of each year. The compliance report must assess the adequacy of internal controls, documentation, and implementation processes to ensure conformity with statewide IT governance, security, and performance standards.

The CIG must provide a consolidated report summarizing agency performance, findings, and recommendations for improvement, and agency heads not under the jurisdiction of the Governor must provide agency reports, to the Executive of the Governor, President of the Senate, and the Speaker of the House of Representatives by December 1 of each year.

Section 5 conforms to changes in the bill by replacing the DMS with the DIGIT in s. 97.0525, F.S., relating to development of the risk assessment methodology.

Section 6 conforms to changes in the bill by replacing the DMS with the DIGIT in s. 112.22, F.S., relating to the identification of prohibited applications.

Section 7 amends s. 119.0725, F.S., to make technical, conforming changes. 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 FLDS to the DIGIT.

Section 8 amends s. 216.023, F.S., to remove the requirement 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 as that information will be included within annual reporting by the DIGIT. It also updates a cross-reference from s. 282.0051, F.S., to s. 282.0061, F.S.

Section 9 amends s. 282.0041, F.S., to provide the following definitions of terms:
- "Agency assessment" is repealed.
- "Customer entity" means an entity that obtains services from the DIGIT.
- "DIGIT" means the Division of Integrated Government Innovation and Technology within the Executive Office of the Governor.
- "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.
- "Project oversight" means an independent review and assessment of an IT project.
- "Risk assessment" means the process of identifying operational and security risks.

Section 10 amends s. 282.00515, F.S., related to Cabinet duties to conform cross-references to amendments made by the bill. In addition, this section adds industry recognized best practices, processes, and methodologies to standards and requires them to enable open data exchange, interoperability, and vendor-neutral system integration. It requires alternative adoption of said standards, practices, processes, and methodologies to be evaluated on a case-by-case basis. It also requires the Cabinet agencies to use the standards established by the DIGIT for enterprise projects that measurably impact another state agency. Additionally, it requires Cabinet agencies to:
- Conduct full baseline needs assessments;
- Produce a phased roadmap that must be submitted annually with legislative budget requests;
- Use the IT reports developed by the DIGIT;
- Report to the Legislature by December 15 of each year the IT financial data required in section 11 of the bill; and
- Consult with the DIGIT if an IT project implemented by a state agency will interface with a Cabinet agency's IT system.

Section 11 creates s. 282.006, F.S., to assign duties and enterprise responsibilities to the DIGIT. The bill provides the DIGIT 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 DIGIT, 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 DIGIT is tasked with the following duties and responsibilities:

- Establishing the strategic direction of IT for state agencies.
- 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 architecture, 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 DIGIT must produce the following reports and provide them to the Governor, the President of the Senate, and the Speaker of the House of Representatives:

- Annually by December 15, an enterprise analysis report for state agencies 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 DIGIT 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 totals:
    - 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 IT staff augmentation.
    - Number of contracts and purchase orders and total amount of associated expenditures for IT 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.
  - 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 IT 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 DIGIT must produce a strategic plan based on the market analysis for the use and implementation of continued and future IT services.

The DIGIT is also tasked 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 must be accessible to all state agencies, including Cabinet agencies, through a secure authentication system, featuring a structured index and search functionality to facilitate the efficient retrieval of information.

The library must be regularly updated to reflect current state and federal requirements, industry best practices, and emerging technologies. It must include standardized checklists organized by

technical subject areas to assist agencies in measuring compliance with IT policies, standards, and best practices.

The DIGIT is required to establish procedures to ensure the integrity, security, and availability of the library, including access controls, encryption, and disaster recovery measures. The DIGIT must 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 DIGIT 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.

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

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

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

The bill requires the baseline needs assessments for state agencies be completed by January 1, 2029, and use the Capability Maturity Model[57] for measuring each agency's IT capabilities, providing a maturity level rating for each assessed domain. Once completed, the assessments must be maintained and updated on a regular schedule adopted by the DIGIT. The DIGIT must submit a plan and schedule to complete the baseline needs assessments to the Governor, the President of the Senate, and the Speaker of the House of Representatives by October 1, 2027. The needs assessments must include documentation of each agency's:

- Distinct technical environments;

[57] 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.

- Existing technical debt;
- Security risks; and
- Compliance with all IT standards and guidelines developed and published by the DIGIT.

In assessing the existing technical debt portion of the needs assessment, the DIGIT must analyze the state's legacy IT 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 IT system, resources, security, and data management to support operations; and
- Any other information necessary for fiscal or technology planning.

State agencies are required to provide all necessary documentation to enable accurate reporting on legacy systems and, with support from the DIGIT, 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 the following be considered and included in the DIGIT's annual enterprise analysis 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 IT services that are common across all state agencies and that support improved:
  - Interoperability;
  - Security;
  - Scalability;
  - Maintainability;
  - Cost efficiency;
  - Business functions; and
  - Operations, including administrative functions such as purchasing, accounting and reporting, cash management, and personnel.

The DIGIT must also review all agency IT legislative budget requests for compliance with IT standards and report findings to the Governor for funding decisions in the Governor's recommended budget.

Additionally, the DIGIT 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 President of the Senate, and the Speaker of the House of Representatives by December 1, 2029. The report must include the vision, goals, and benefits of implementing a statewide master data management initiative, an analysis of the current state, and the recommended strategy, methodology, and estimated timeline and resources needed at a state agency and enterprise level to accomplish the initiative.

The DIGIT 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, methodologies, and oversight measures for IT project planning and implementation that objectively provide data regarding the project progress and risks, 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.
- Creating a framework with processes, activities, and deliverables state agencies must comply with when planning an IT project.
- Developing standardized IT project reporting templates for use by state agencies.
- Providing project management and oversight training to state agencies that must be reevaluated every two years.
- Performing project oversight on projects with a total project cost of $10 million or more and reporting quarterly on any IT project that DIGIT identifies as high-risk to include a list of all projects with outstanding performance deviancies.
- Establishing a streamlined reporting process with clear timelines and procedures to notify a state agency if there is deviation from the adopted standards.

The DIGIT is required to develop standardized, category-based performance standards and measurable metrics to evaluate information technology vendors providing commodities or services to the state. It requires DIGIT to establish a scoring mechanism to inform procurement and contract management decisions, create a publicly available preferred vendors list with vendor rankings, and provide for priority consideration in future procurements based on performance and cost. The standards and scoring methodology must be periodically reviewed and updated to reflect evolving technology and state needs.

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

State agencies must work with the DIGIT to establish alternative standards and policies if adherence to standards or policies published by the DIGIT 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., to establish multiple enterprise-level IT workgroups within the DIGIT 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 DIGIT leadership on key areas such as cybersecurity, data interoperability, quality assurance, project management, and purchasing. Additionally, state IT leaders, including the CIO, Chief Information Security Officer, Chief Data Officer, Chief

Technology Officer, Chief Technology Procurement Officer, and others will consult with these workgroups on a quarterly basis to ensure continuous improvement in IT governance and strategy.

Section 14 creates s. 282.0063, F.S., to address the DIGIT's role in IT workforce development. The DIGIT 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 DIGIT must 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 DIGIT must also create a statewide training program to help agencies implement enterprise architecture policies and standards. Additionally, the DIGIT 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 DIGIT must establish internship and scholarship-for-service programs.

Section 15 creates 282.0064, F.S., to define the DIGIT's responsibilities related to IT contracts and procurements. The DIGIT must coordinate with the DMS to 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 DIGIT will coordinate with the DMS to evaluate responses and answer vendor questions for IT related state term contracts. Cabinet agencies are permitted to adopt alternative standards but must notify the Governor and the Legislature and provide a justification for adoption of the alternatives to include how the agency will meet the IT policy.

Section 16 amends s. 282.318, F.S., by naming the DIGIT as the lead entity responsible for establishing enterprise technology and cybersecurity standards that are aligned with generally accepted technology best practices, and replacing remaining references to the FLDS. It removes the responsibilities for the operation and maintenance of a Cybersecurity Operations Center (CSOC) and leading an Emergency Support Function, ESF CYBER, under the state comprehensive emergency management plan.

The bill provides for incident reporting to and through the state chief information security officer in place of the cybersecurity operations center; adds a provision to report incidents to the Northwest Regional Data Center (NWRDC), if applicable; 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 17 amends, and makes technical, conforming changes to s. 282.3185, F.S., related to local government cybersecurity. The state chief information security officer will now receive incident reports in place of the FLDS and the CSOC. The bill also deletes references to the Cybersecurity Advisory Council (CAC).

The DIGIT 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 18 repeals s. 282.319, F.S., related to the CAC. These activities will generally be within the scope of the DIGIT duties and responsibilities.

Section 19 deletes obsolete language in s. 282.201, F.S., related to the DMS management of the state data center, requires the 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 included in ch. 2025-199, L.O.F.

Section 20 creates s. 282.2011, F.S., regarding the state data center services provided by the NWRDC to move data center provisions 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 21 amends s. 282.206, F.S., to add the DIGIT and the NWRDC as recipients of the state agency strategic plan for applications located at the state data center, and to require state agencies also provide documentation of the feasibility and appropriateness of moving applications to the cloud to better align with s. 282.206(1), F.S.

Section 22 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 23 creates s. 287.0583, F.S., to require IT contracts include provisions ensuring data portability, operational documentation, transition support, and total cost of ownership.

Section 24 amends s. 287.0591, F.S., to require the DIGIT, instead of the FLDS, to coordinate with the DMS in the process for technology state term contract solicitations, and specifies the minimum coordination activities. It changes the distribution requirement for a request for quote to a minimum number of approved vendors to only those with a threshold amount of at least category two but less than category four and requires agencies to maintain a copy of a request for quote for two years after a purchase order is issued.

The bill also adds a requirement that a request for quote to purchase IT commodities, consultant services, or staff augmentation contractual services from the state term contract which exceeds the category four threshold amount is subject to the public records requirements per s. 287.057, F.S., and requiring agencies to:

- Publish the request for quote for at least ten days before a purchase order is issued;
- Publish the name of the vendor awarded the purchase order; and
- Maintain a copy of the request for quote, the vendor that was sent the request for quote, and any vendor responses for two years after a purchase order is issued.

The amended language specifies that a decision resulting from a request for quote is not subject to protest under s. 120.57(3), F.S., and allows the DMS to prequalify vendors for IT commodities on state term contract.

Section 25 abolishes the FLDS within the DMS in s. 20.22, F.S.

Section 26 amends s. 282.802, F.S., to transfer the Government Technology Modernization Council from the DMS to the DIGIT, names the CIO as the nonvoting executive director of the council, and make other conforming changes.

Section 27 amends s. 282.604, F.S., by transitioning rulemaking authority regarding accessible electronic information technology by governmental units from the DMS to the DIGIT.

Section 28 requires the Department of Commerce to consult with the DIGIT in place of the FLDS regarding the Reemployment Assistance Claims and Benefits Information System in s. 443.1113, F.S.

Section 29 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.

Section 30 deletes the requirement that a request for assistance with a cybersecurity incident must come from the FLDS in s. 1004.444, F.S.

Section 31 provides that the bill takes effect January 5, 2027.

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 establishes the Division of Integrated Government Innovation and Technology (DIGIT) under the Executive Office of the Governor. The fiscal impact for Fiscal Year 2026-2027 is zero. Existing resources will transfer from the Florida Digital Services (FDS) to the DIGIT to support the cost of the DIGIT.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 20.055, 97.0525, 112.22, 119.0725, 216.023, 282.0041, 282.00515, 282.318, 282.3185, 282.201, 282.206, 1004.649, 20.22, 282.802, 282.604, 287.0591, 443.1113, 943.0415, and 1004.444.

This bill creates the following sections of the Florida Statutes: 14.205, 282.006, 282.0061, 282.0062, 282.0063, 282.0064, 282.2011, and 287.0583.

This bill repeals section 282.319 of the Florida Statutes.

IX. Additional Information:

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

CS/CS by Appropriations on February 12, 2026:
The committee substitute requires DIGIT to develop and maintain standardized standards, performance metrics, and evaluation tools to assess information technology vendors providing commodities or services to the state. The standards must be organized by vendor category and include objective, measurable criteria such as timeliness, quality, cost control, contract compliance, security practices, and customer satisfaction. The framework must allow for the collection and analysis of performance data across agencies to ensure consistent evaluations. It establishes a scoring mechanism that may be used in procurement and contract management, supports the creation of a publicly available preferred vendors list with rankings by category, and provides that, to the extent permitted by law, priority consideration in future procurements be based on performance ranking and cost. The standards and methodology must be periodically reviewed and updated.

It also incorporates existing statutory provisions applicable to the state data center regarding equipment custodianship and administrative access to ensure Criminal Justice Information System (CJIS) compliance.

CS by Appropriations Committee on Agriculture, Environment, and General Government on February 4, 2026:
The committee substitute:
- Provides for the selection of a state chief technology officer and a state chief technology procurement officer.
- Clarifies the duties of the agency inspectors general to focus on information technology reporting, project, contract, and procurement standards.
- Specifies the Division of Integrated Government Innovation and Technology (DIGIT) is within the Executive Office of the Governor.
- Replaces “analysis” with “assessment” in the definition of project oversight and adds “operational risk” to the definition of risk assessment.
- Requires Cabinet agencies to adopt standards based on industry-recognized best practices, and to enable open data exchange and vendor-neutral system integration.

- Requires the DIGIT to review agency legislative budget requests for compliance with information technology (IT) standards and provide the results to the Executive Office of the Governor for consideration of funding decisions in the Governor's recommended budget.
- Specifies provisions in s. 282.0061(5)(d) pertain to IT project planning and implementation, including:
  - Performance metrics to measure whether a project is delivering intended outcomes;
  - Thresholds to guide corrective actions relating to project complexity, scale, performance, and quality;
  - Procedures for timely engaging and notifying stakeholders when acceptable variances are exceeded and escalating critical issues to appropriate individuals; and
  - Development of a planning framework to be used by state agencies for IT projects.
- Requires the DIGIT to develop training specific to project management and oversight that must be reevaluated every two years.
- Establishes a high-risk designation trigger for projects with a total cost exceeding $10 million and requires inclusion of identified project performance deficiencies in the quarterly project oversight report.
- Changes the title of the state chief information technology officer to the state chief technology officer.
- Defines the DIGIT's coordination activities with the Department of Management Services (DMS) on state-term contract procurements.
- Ensures cybersecurity standards remain up to date, by requiring the risk assessment methodology to align with National Institute for Standards and Technology Cybersecurity Framework and allowing agencies to use independent third-party vendors to perform the risk assessments that must be submitted to DIGIT.
- Defines the state data center reporting elements required by the Northwest Regional Data Center.
- Includes documentation of the feasibility and appropriateness of moving applications to the cloud to better align with s. 282.206(1), F.S.
- Requires IT contracts ensure data portability, operational documentation, transition support, and the total cost of ownership.
- Require the DMS to coordinate with the DIGIT when issuing procurements for IT commodities, consultant services, or staff augmentation contractual services.
- Changes the distribution requirement for a request for quote to a minimum number of approved vendors to only those with a value of at least category two but less than category four and require agencies to maintain a copy of a request for quote for two years after a purchase order is issued.
- Adds a requirement that a request for quote with a value over category four is subject to the public records requirements per s. 287.057, F.S., and requiring agencies to:
  - Publish the request for quote for at least ten days before a purchase order is issued;
  - Publish the name of the vendor awarded the purchase order; and

- Maintain a copy of the request for quote, the vendor that was sent the request for quote, and any vendor responses for two years after a purchase order is issued.
- Specifies that a decision resulting from a request for quote is not subject to protest.
- Allows the DMS to prequalify vendors for IT commodities on state term contract.

B. Amendments:

None.

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