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 Governmental Oversight and Accountability

BILL:	CS/SB 1708
INTRODUCER:	Governmental Oversight and Accountability Committee and Senator DiCeglie
SUBJECT:	Cybersecurity
DATE:	March 30, 2023 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Harmsen	McVaney	GO	**Fav/CS**
2.			AEG	
3.			AP	
4.			RC	

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 1708, which may be called the "Florida Cyber Protection Act," makes several changes to laws regarding state information technology and cybersecurity governance. The bill:

- Requires the Department of Management Services (DMS), through the Florida Digital Service (FLDS), to ensure independent oversight of state agency IT procurements;
- Establishes an operations committee that will develop collaborative efforts between agencies and other governmental entities relating to cybersecurity issues;
- Creates the position of state chief technology officer, who will explore technology solutions, and support cybersecurity and interoperability initiatives, among other duties;
- Expands oversight and management duties of the state data center, and grants the FLDS full access to its infrastructure;
- Provides that the state data center, or its successor entity, must fully integrate with the Cybersecurity Operations Center;
- Requires agencies and local governments to notify the FLDS of any cybersecurity or ransomware incident;
- Grants the FLDS the ability to respond to any state agency cybersecurity incident; and
- Allows the FLDS to brief members of a legislative committee or subcommittee that is responsible for cybersecurity issues

The state chief information officer (CIO), who serves as head of the FLDS, will now be appointed by the Governor and subject to Senate confirmation.

The bill provides that local governments and private businesses cannot be liable for torts related to cybersecurity breaches if they adhere to specific cybersecurity protocol, and update their protocol according to provisions adopted in the bill.

The bill does not have a fiscal impact on state or local government revenues or local government expenditures. The bill may increase state expenditures.

The bill takes effect on July 1, 2023.

II. Present Situation:

State Information Technology Management

The Department of Management Services (DMS) oversees information technology (IT) governance and security for the executive branch of the State government.[1] The Florida Digital Service (FLDS) within the DMS was established by the Legislature in 2020[2] to replace the Division of State Technology. The FLDS works subordinate to the DMS to implement policies for IT and agency cybersecurity, and to fully support Florida's cloud first policy.[3]

The FLDS was created to modernize state government technology and information services.[4] Accordingly, 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 that facilitates interoperability between agencies and supports the cloud-first policy;
- Establish IT project management and oversight standards for state agencies;
- Oversee state agency IT projects that cost $10 million or more and that are funded in the General Appropriations Act or any other law;[5] and
- Standardize and consolidate IT services that support interoperability, Florida's cloud first policy, and other common business functions and operations.

The head of FLDS is appointed by the Secretary of DMS and serves as the state chief information officer (CIO).[6] The CIO must have at least 5 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.[7]

[1] Section 282.0051, F.S.
[2] Ch. 2020-161, Laws of Fla.
[3] Section 282.0051(1), F.S.
[4] Section 282.0051(1), F.S.
[5] The FLDS provides project oversight on IT projects that have a total cost of $20 million or more for the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services. Section 282.0051(1)(m), F.S.
[6] Section 282.0051(2)(a), F.S.
[7] *Id*.

State Data Center

Present Situation

In 2022 the State Data Center (SDC) was moved from FLDS to DMS, which now operates and maintains the SDC.[8] The SDC provides data center services that comply with applicable state and federal laws, regulations, and policies, including all applicable security, privacy, and auditing requirements.[9] The standards used by the SDC are created through the Information Technology Infrastructure Library (ITIL); the International Organization for Standardization; and the International Electrotechnical Commission (ISO/IEC) 27,000; and the Project Management Institute's (PMI) best practices.

Northwest Regional Data Center

The Northwest Regional Data Center (NWRDC) is the leading computing provider for educational and governmental communities in Florida. In 2022, NWRDC (located at Florida State University) was declared an official state data center, and the current SDC resources, contracts, and assets were transferred to NWRDC, through contract.[10] This allows for NWRDC to provide services from the SDC facility. The NWRDC offers services and 24/7 management support for various IT support solutions, including: public/private cloud services, backup and recovery, storage, managed services, Tallahassee fiber loop, Florida LambdaRail, MyFloridaNet, Florida Power and Light Fibernet, CenturyLink Connectivity, security services, multi-site colocation, and disaster recovery.[11]

State Cybersecurity Act

Agency Cybersecurity Standards

The State Cybersecurity Act[12] requires the DMS and the heads of state agencies to meet certain requirements to enhance state agencies' cybersecurity.[13] Specifically, the DMS, acting through the FLDS, must:[14]

- Assess state agency cybersecurity risks and determine appropriate security measures consistent with generally accepted best practices for cybersecurity.
- Adopt rules to mitigate risk, support a security governance framework, and safeguard state agency digital assets, data, information, and IT resources[15] to ensure availability, confidentiality, and integrity.
- Designate a chief information security officer (CISO) who must develop, operate, and oversee state technology systems' cybersecurity. The CISO must be notified of all confirmed

[8] Ch. 2022-153, Laws of Fla.
[9] Section 282.201(1), F.S.
[10] Section 282.201(5), F.S.
[11] NWRDC: Florida's Cloud Broker, *About Northwest Regional Data Center*, https://www.nwrdc.fsu.edu/about (last visited Mar. 29, 2023).
[12] Section 282.318, F.S.
[13] "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.
[14] Section 282.318(3), F.S.
[15] "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.

or suspected incidents or threats of state agency IT resources and must report such information to the CIO and the Governor.
- Develop and annually update a statewide cybersecurity strategic plan that includes security goals and objectives for cybersecurity, including the identification and mitigation of risk, proactive protections against threats, tactical risk detection, threat reporting, and response and recovery protocols for cyber incidents.
- Develop a cybersecurity governance framework and publish it for state agency use.
- Assist state agencies in complying with the State Cybersecurity Act.
- Train state agency information security managers and computer security incident response team members, in collaboration with the Florida Department of Law Enforcement (FDLE) Cybercrime Office, on issues relating to cybersecurity, including cybersecurity threats, trends, and best practices.
- Provide cybersecurity training to all state agency technology professionals that develop, assess, and document competencies by role and skill level. The training may be provided in collaboration with the Cybercrime Office, a private sector entity, or an institution of the state university system.
- Annually review state agencies' strategic and operational cybersecurity plans.
- Track, in coordination with agency inspectors general, state agencies' implementation of remediation plans.
- Operate and maintain a Cybersecurity Operations Center led by the CISO to serve as a clearinghouse for threat information and to coordinate with the FDLE to support state agency response to cybersecurity incidents.
- Lead an Emergency Support Function under the state comprehensive emergency management plan.

The State Cybersecurity Act requires the head of each state agency to designate an information security manager to administer the cybersecurity program of the state agency.[16] In addition, agency heads must:
- Establish an agency cybersecurity incident response team, which must report any confirmed or suspected cybersecurity incidents to the CISO.
- Submit an annual strategic and operational cybersecurity plan to the DMS.
- Conduct a triennial comprehensive risk assessment to determine the security threats to the data, information, and IT resources of the state agency.
- Develop and update internal policies and procedures, including procedures for reporting cybersecurity incidents and breaches to the FLDS and the Cybercrime Office.
- Implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended by the DMS to address identified risks to the data, information, and IT resources of the agency.
- Ensure periodic internal audits and evaluations of the agency's cybersecurity program.
- Ensure that cybersecurity contract requirements of IT and IT resources and services meet or exceed applicable state and federal laws, regulations, and standards for cybersecurity, including the NIST cybersecurity framework.
- Provide cybersecurity awareness training to all state agency employees concerning cybersecurity risks and the responsibility of employees to comply with policies, standards,

[16] Section 282.318(4)(a), F.S.

guidelines, and operating procedures adopted by the state agency to reduce those risks. The training may be provided in collaboration with the Cybercrime Office, a private sector entity, or an institution of the state university system.
- Develop a process, consistent with FLDS rules and guidelines, to detect, report, and respond to threats, breaches, or cybersecurity incidents.

Specifically, state agencies and local governments in Florida, must report all ransomware incidents and any cybersecurity incidents at severity levels three, four, and five incident 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, to the Cybersecurity Operations Center.[17] The Cybersecurity Operations Center shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level three, four, or five as soon as possible, but no later than 12 hours after receiving the incident report from the state agency or local government.[18] For state agency and local government incidents at severity levels one and two, they must report these to the Cybersecurity Operations Center and the Cybercrime Office at FDLE as soon as possible.[19]

In addition, the Cybersecurity Operations Center must provide consolidated incident reports to the President of the Senate, Speaker of the House of Representatives, and the Advisory Council on a quarterly basis.[20]

State agencies and local governments must also submit an after-action report to FLDS within 1 week of the remediation of a cybersecurity or ransomware incident.[21] The report must summarize the incident, state the resolution, and provide any insights from the incident.

Public Record and Public Meetings Exemption for Specific Cybersecurity Records Held by Agencies

The State Cybersecurity Act makes confidential and exempt from public records copying and inspection requirements the portions of risk assessments, evaluations, external audits, and other agency cybersecurity program reports that are held by an agency, if the disclosure would facilitate unauthorized access to, modification, disclosure, or destruction of data or IT resources.[22] However, this information must be shared with the Auditor General, DLE Cybercrime Office, FLDS, and the Chief Inspector General. An agency may share its confidential and exempt documents with a local government, another agency, or a federal agency if given for a cybersecurity purpose, or in furtherance of the agency's official duties.[23]

The State Cybersecurity act also exempts portions of any public meeting that would reveal records that it makes confidential and exempt.[24]

[17] Sections 282.318(3)(c)9.c, and 282.3185(5)(b)1., F.S.
[18] Sections 282.318(3)(c)9.c.(II), and 282.3185(5)(b)2. F.S.
[19] Sections 282.318(3)(c)9.d., 282.3185(5)(c), F.S.
[20] Sections 282.318(3)(c)9.e, and 282.3185(5)(d), F.S.
[21] Sections 282.318(4)(k), and 282.3185(6), F.S. *See also*, ch. 2022-220, Laws of Fla.
[22] Section 282.318(5), F.S.
[23] Section 282.318(7), F.S.
[24] Section 282.318(6), F.S.

Florida Cybersecurity Advisory Council

The Florida Cybersecurity Advisory Council (Advisory Council) within the DMS[25] protects IT resources from cyber threats and incidents.[26]

The Advisory Council's membership must consist of:
- The Lieutenant Governor or his or her designee.
- The state chief information officer.
- The state chief information security officer.
- The director of the Division of Emergency Management or his or her designee.
- A representative of the computer crime center of the Department of Law Enforcement, appointed by the executive director of the Department of Law Enforcement.
- A representative of the Florida Fusion Center of the Department of Law Enforcement, appointed by the executive director of the Department of Law Enforcement.
- The Chief Inspector General.
- A representative from the Public Service Commission.
- Up to two representatives from institutions of higher education located in this state, appointed by the Governor.
- Three representatives from critical infrastructure sectors, one of whom must be from a water treatment facility, appointed by the Governor.
- Four representatives of the private sector with senior level experience in cybersecurity or software engineering from within the finance, energy, health care, and transportation sectors, appointed by the Governor.
- Two representatives with expertise on emerging technology, with one appointed by the President of the Senate and one appointed by the Speaker of the House of Representatives.

The Advisory Council must assist the FLDS with the implementation of 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.[27] The Advisory Council meets at least quarterly to:[28]
- 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.
- Develop cybersecurity best practice recommendations for state agencies, including continuous risk monitoring, password management, and protecting data in legacy and new systems.
- Examine inconsistencies between state and federal law regarding cybersecurity.

[25] Section 282.319(1), F.S.
[26] Section 282.319(2), F.S.
[27] Section 282.319(3), F.S. The Cybersecurity Task Force is no longer active. *See*, Florida DMS, *Cybersecurity Task Force Overview*, https://www.dms.myflorida.com/other_programs/cybersecurity_advisory_council/cybersecurity_task_force (last visited Mar. 29, 2023).
[28] Section 282.319(9), F.S.

Beginning June 30, 2022, and each June 30 thereafter, the Advisory Council must submit cybersecurity recommendations to the Legislature.[29]

Limitation on Liability

Tort Liability and Negligence

A tort is a civil legal action to recover damages for a loss, injury, or death due to the conduct of another. Some have characterized a tort as a civil wrong, other than a claim for breach of contract, in which a remedy is provided through damages.[30] When a plaintiff files a tort claim, he or she alleges that the defendant's "negligence" caused the injury. Negligence is defined as the failure to use reasonable care. It means the care that a reasonably careful person would use under similar circumstances. According to the Florida Standard Jury Instructions, negligence means "doing something that a reasonably careful person would not do" in a similar situation or "failing to do something that a reasonably careful person would do" in a similar situation.[31]

When a plaintiff seeks to recover damages for a personal injury and alleges that the injury was caused by the defendant's negligence, the plaintiff bears the legal burden of proving that the defendant's alleged action was a breach of the duty that the defendant owed to the plaintiff.[32]

Negligence Pleadings

To establish a claim for relief and initiate a negligence lawsuit, a plaintiff must file a "complaint." The complaint must state a cause of action and contain: a short and plain statement establishing the court's jurisdiction, a short and plain statement of the facts showing why the plaintiff is entitled to relief, and a demand for judgment for relief that the plaintiff deems himself or herself entitled. The defendant responds with an "answer," and provides in short and plain terms the defenses to each claim asserted, admitting or denying the averments in response.[33]

Under the Florida Rules of Civil Procedure, there is a limited group of allegations that must be pled with "particularity." These allegations include allegations of fraud, mistake, and a denial of performance or occurrence.[34]

Four Elements of a Negligence Claim

To establish liability, the plaintiff must prove four elements:
- Duty – That the defendant owed a duty, or obligation, of care to the plaintiff;
- Breach – That the defendant breached that duty by not conforming to the standard required;
- Causation – That the breach of the duty was the legal cause of the plaintiff's injury; and
- Damages – That the plaintiff suffered actual harm or loss.

[29] Section 282.319(11), F.S.
[30] BLACK'S LAW DICTIONARY (11th ed. 2019).
[31] Fla. Std. Jury Instr. Civil 401.3, *Negligence*.
[32] Florida is a comparative negligence jurisdiction as provided in s. 768.81(2), F.S. In lay terms, if a plaintiff and defendant are both at fault, a plaintiff may still recover damages, but those damages are reduced proportionately by the degree that the plaintiff's negligence caused the injury.
[33] Fla. R. Civ. P. 1.110.
[34] Fla. R. Civ. P. 1.120(b) and (c).

Burden or Standard of Proof

A "burden of proof" is the obligation a party bears to prove a material fact. The "standard of proof" is the level or degree to which an issue must be proved.[35] The plaintiff carries the burden of proving, by a specific legal standard, that the defendant breached the duty that was owed to the plaintiff that resulted in the injury. In civil cases, two standards of proof generally apply:

- The "greater weight of the evidence" standard, which applies most often in civil cases, or
- The "clear and convincing evidence" standard, which applies less often, and is a higher standard of proof.[36]

However, there are certain statutory and common law presumptions[37] that may shift the burden of proof from the party asserting the material fact in issue to the party defending against such fact.[38] These presumptions remain in effect following the introduction of evidence rebutting the presumption, and the factfinder must decide if such evidence is strong enough to overcome the presumption.[39] A presumption is a legal inference that can be made with knowing certain facts. Most presumptions are able to be rebutted, if proven to be false or thrown into sufficient doubt by the evidence.[40]

Greater Weight of the Evidence

The greater weight of the evidence standard of proof means "the more persuasive and convincing force and effect of the entire evidence in the case."[41] Some people explain the "greater weight of the evidence" concept to mean that, if each party's evidence is placed on a balance scale, the side that dips down, even by the smallest amount, has met the burden of proof by the greater weight of the evidence.

Clear and Convincing

The clear and convincing standard, a higher standard of proof than a preponderance of the evidence, requires that the evidence be credible and the facts which the witness testifies to must be remembered distinctly. The witness's testimony "must be precise and explicit and the witnesses must be lacking in confusion as to the facts in issue." The evidence must be so strong that it guides the trier of fact to a firm conviction, to which there is no hesitation, that the allegations are true.[42]

Standards of Care and Degrees of Negligence

Courts have developed general definitions for the degrees of negligence.

[35] 5 Fla. Prac. Civil Practice s. 17.1, (2023 ed.)
[36] *Id*.
[37] These presumptions tend to be social policy expressions, such as the presumption that all people are sane or that all children born in wedlock are legitimate. 5 *Florida Practice Series* s. 16:1.
[38] 5 *Florida Practice Series* s. 16:1.
[39] *Id.*
[40] Legal Information Institute, *Presumption*, https://www.law.cornell.edu/wex/presumption (last visited Mar. 29, 2023).
[41] Fla. Std. Jury Instr. 401.3, *Greater Weight of the Evidence*.
[42] *Slomowitz v. Walker*, 429 So. 2d 797, 800 (Fla. 4th DCA 1983).

Slight Negligence	The failure to exercise great care.[43]
Ordinary Negligence or Simple Negligence	The conduct that a reasonable and prudent person would know might result in injury to others.[44]
Gross Negligence	A course of conduct which a reasonable and prudent person knows would probably and most likely result in injury to another.[45] To prove gross negligence, a plaintiff must show: circumstances that, when taken together, create a clear and present danger; an awareness that the danger exists; and a conscious, voluntary act or omission to act that will likely result in an injury.

Florida Information Protection Act (FIPA)[46]

FIPA is a data security measure that requires governmental entities, specific business entities, and any third-party agent that holds or processes personal information on behalf of these entities to take reasonable measures to protect a consumer's personal information. Additionally, FIPA requires covered business entities[47] that are subject to data breaches to attempt to remediate the breach by notification to affected consumers in Florida, and in cases where more than 500 individual's information was breached—by additional notification to the Department of Legal Affairs (DLA).[48] If the breach affected more than 1,000 individuals in Florida, the entity must also notify credit reporting agencies, with certain exceptions.[49]

FIPA defines "personal information" as:

- Online account information, such as security questions and answers, email addresses, and passwords; and
- An individual's first name or first initial and last name, in combination with any one or more of the following information regarding him or her:
  - A social security number;
  - A driver license or similar identity verification number issued on a government document;
  - A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

[43] *See Faircloth v. Hill*, 85 So. 2d 870 (Fla. 1956); *see also Holland America Cruises, Inc. v. Underwood*, 470 So. 2d 19 (Fla. 2d DCA 1985); *Werndli v. Greyhound Corp.*, 365 So. 2d 177 (Fla. 2d DCA 1978); 6 *Florida Practice Series* s. 1.2.
[44] *See De Wald v. Quarnstrom*, 60 So. 2d 919 (Fla. 1952); *see also Clements v. Deeb*, 88 So. 2d 505 (Fla. 1956); 6 *Florida Practice Series* s. 1.2.
[45] *See Clements*, 88 So. 2d 505; 6 *Florida Practice Series* s. 1.2.
[46] Section 501.171, F.S.; Chapter 2014-189, Laws of Fla. (FIPA expanded and updated Florida's data breach disclosure laws contained in s. 817.5681, F.S. (2013), which was adopted in 2005 and repealed in 2014).
[47] A "covered entity" is a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. Section 501.171(1)(b), F.S.
[48] Florida Office of the Attorney General (OAG), *How to Protect Yourself: Data Security*, http://myfloridalegal.com/pages.nsf/Main/53D4216591361BCD85257F77004BE16C (last visited Mar. 29, 2023). Section 501.171(3)-(4), F.S.
[49] Section 501.171(3)-(6), F.S.

- Medical history information or health insurance identification numbers; or
- An individual's health insurance identification numbers.[50]

Personal information does not include information:

- About an individual that a federal, state, or local governmental entity has made publicly available; or
- That is encrypted, secured, or modified to remove elements that personally identify an individual or that otherwise renders the information unusable.[51]

FIPA does not provide a private cause of action, but authorizes the DLA to file charges against covered entities under Florida's Unfair and Deceptive Trade Practices Act (FDUTPA).[52]

In addition to the remedies provided for under FDUTPA, a covered entity that fails to notify the DLA, or an individual whose personal information was accessed, of the data breach is liable for a civil penalty of $1,000 per day for the first 30 days of any violation; $50,000 for each subsequent 30-day period of violation; and up to $500,000 for any violation that continues more than 180 days. These civil penalties apply per breach, not per individual affected by the breach.

Cybersecurity Standards

Local governments are required to adopt cybersecurity standards that safeguard the local government's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity.[53] The standards must be consistent with generally accepted best practices for cybersecurity, including the NIST cybersecurity framework.[54] Once it adopts the standards, the local government must notify FLDS as soon as possible.[55]

The National Institute for Standards and Technology (NIST) is a non-regulatory federal agency housed within the U.S. Department of Commerce. NIST is charged with providing a prioritized, flexible, repeatable, performance-based, and cost-effective framework that helps owners and operators of critical infrastructure identify, assess, and manage cyber risk. While the framework was developed with critical infrastructure in mind, it can be used by organizations in any sector of the economy or society.[56] The framework is designed to complement an organization's own approach to cybersecurity risk management. As such, there are a variety of ways to use the framework and the decision about how to apply it is left to the implementing organization. For example, an organization may use its current processes and consider the framework to identify opportunities to strengthen its cybersecurity risk management. The framework, overall, provides an outline of best practices that helps organizations decide where to focus resources for cybersecurity protection.[57] Other cybersecurity standards include:

[50] Section 501.171(1)(g)1., F.S.; OAG *supra* note 41.
[51] Section 501.171(1)(g)2., F.S.
[52] Section 501.171(9), (10), F.S.; OAG *supra* note 41.
[53] Section 282.3185(4)(a), F.S.
[54] *Id*.
[55] Section 282.3185(4)(d), F.S.
[56] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited March 29, 2023).
[57] *Id*.

NIST special publication 800-171	Provides recommended requirements for protecting the confidentiality of controlled unclassified information. If a manufacturer is part of a Department of Defense, General Services Administration, NASA, or other state or federal agency supply chain then they must comply with these security requirements.[58]
NIST special publications 800-53 and 800-53A	A category of security and privacy controls. Covers the steps in the Risk Management Framework that address security controls for federal information systems.[59]
The Federal Risk and Authorization Management Program security assessment framework	Organization established by the General Services Administration (a Federal Government Program) that provides U.S. federal agencies, state agencies, and their vendors with a standardized set of best practices to assess, adopt, and monitor the use of cloud-based technology services under the Federal Information Security Management Act (FISMA).[60]
CIS Critical Security Controls	The Center for Internet Security Critical Security Controls (CIS) are a prescriptive and simplified set of best practices for strengthening cybersecurity for different organizations. CIS was created in response to extreme data losses experienced by organizations in the U.S. defense industrial base.[61]
The International Organization for Standardization/International Electrotechnical Commission 27000 – series family of standards	ISO/IEC 27001 (ISO) enables organizations of all sectors to manage security of financial information, intellectual property, employee data and information entrusted by third parties. ISO has auditors and is an international standard. There are 804 technical committees and subcommittees concerned with such standards of development.[62]

[58] NIST, *What is the NIST SP 800-171 and Who Needs to Follow It?*, https://www.nist.gov/blogs/manufacturing-innovation-blog/what-nist-sp-800-171-and-who-needs-follow-it-0#:~:text=NIST%20SP%20800-171%20is%20a%20NIST%20Special%20Publication,protecting%20the%20confidentiality%20of%20controlled%20unclassified%20information%20%28CUI%29 (last visited Mar. 29, 2023).
[59] NIST, *Selecting Security and Privacy Controls: Choosing the Right Approach*, https://www.nist.gov/blogs/cybersecurity-insights/selecting-security-and-privacy-controls-choosing-right-approach (last visited Mar. 29, 2023).
[60] Reciprocity, *How State and Local Agencies Can Use FedRAMP*, https://reciprocity.com/how-state-and-local-agencies-can-use-fedramp/#:~:text=The%20Federal%20Risk%20and%20Authorization%20Management%20Program%20%28FedRAMP%29,cloud%20products%20offered%20by%20cloud%20service%20providers%20%28CSPs%29 (last visited Mar. 29, 2023).
[61] CIS Security, *CIS Critical Security Controls*, https://www.cisecurity.org/controls (last visited Mar. 29, 2023).
[62] ITGovernance, *ISO 27001, The International Security Standard*, https://www.itgovernanceusa.com/iso27001#:~:text=ISO%2027001%20is%20a%20globally%20recognized%20information%20security,trusted%20benchmark.%20Protect%20your%20data%2C%20wherever%20it%20lives (last visited Mar. 29, 2023).

III. Effect of Proposed Changes:

IT Project Oversight

Section 4 amends s. 282.0051, F.S., to require the DMS, acting through the FLDS, to provide *independent*[63] oversight of state agency IT projects that cost $10 million or more. Specifically:

- The DMS cannot provide project oversight if it has provided, or may be asked to provide, any operational or technical advice on the project, including advice and review. However, it can procure project oversight for agencies and other entities;
- The DMS must create a form contract that state agencies, the DLA, DFS, and DACS[64] can use to procure project oversight services;
- Independent entities that provide project oversight must submit a project oversight report to the DMS; and
- The DMS, acting through the FLDS, must compile the project oversight reports it receives on a quarterly basis and submit a report to the Governor, President of the Senate, and Speaker of the House of Representatives.

Operations Committee

Section 4 also creates an operations committee within the FLDS that will develop collaborative efforts regarding cybersecurity issues between agencies, including agency responses to cybersecurity incidents and interoperability of agency projects. The Secretary of the DMS will serve as the committee's executive director, and the committee's membership will consist of:

- The Attorney General, or his or her designee;
- The Secretary of State, or his or her designee;
- The executive director of the Department of Law Enforcement, or his or her designee;
- The Secretary of Transportation, or his or her designee;
- The director of the Division of Emergency Management, or his or her designee;
- The Secretary of Health Care Administration, or his or her designee;
- The Commissioner of Education, or his or her designee;
- The executive director of the Department of Highway Safety and Motor Vehicles, or his or her designee;
- The chair of the Public Service Commission, or his or her designee;
- The director of the Florida State Guard, or his or her designee;
- The adjutant General of the Florida National Guard, or his or her designee; and
- Any other agency head appointed by the Governor.

Appointments

Section 4 also removes the DMS Secretary's authority to appoint the FLDS CIO, and gives that authority to the Governor, subject to confirmation by the Senate.

---

[63] Section 3 of the bill defines "independent" as, for an entity providing independent verification and validation, having no technical, managerial, or financial interest in the relevant technology project; no relationship to the relevant agency; and no responsibility for or participation in any aspect of the project, which includes project oversight by the Florida Digital Service."

[64] These entities, combined, are defined as the "enterprise" for the purposes of ch. 282, F.S. See s. 282.0041(15), F.S.

The bill removes the CIO's duty to consult with the DMS' Secretary to designate a state chief data officer.

Section 4 of the bill creates the position of state chief technology officer (CTO), who is responsible for:
- Exploring technology solutions to meet the enterprise's needs;
- The deployments of adopted enterprise solutions;
- Compliance with the cloud-first policy, for which the CTO may acquire cloud migration services;
- Recommending best practices to increase technology project success;
- Developing strategic partnerships with the private sector; and
- Directly supporting enterprise cybersecurity and data interoperability initiatives.

The CIO will designate the CTO.

State Data Center

Section 5 amends s. 282.201, F.S., to add additional oversight structure to the state data center. Pursuant to the bill, the data center will be overseen and accountable to the DMS, in consultation with the CIO, state chief data officer, CISO, and CTO. The CIO will appoint the director of the data center.

If the data center will procure or purchase enterprise architecture that would be comparable to a project subject to oversight pursuant to s. 282.0051(4), F.S., if the cost will be $10 million or more, and that may be consumed by an enterprise, then the data center must provide the procurement or purchase documents to the DMS and the FLDS before its publication.

As an additional function of this oversight, the bill grants the CIO authority to assume responsibility for the Northwest Regional Data Center contract, and states that "notwithstanding the terms of the contract" the Northwest Regional Data Center must provide the FLDS with access to information regarding its operation of the state data center.

The bill creates an additional subsection that requires the state data center and any successor entity, including but not limited to the Northwest Regional Data Center, to give the FLDS full access to any infrastructure, system, application, or other means that hosts, supports, or manages data held by a state agency or other enterprise member. The state data center or its successor must fully integrate with the Cybersecurity Operations Center.

Lastly, the state data center or its successor must submit a quarterly report to the FLDS that provides the number of:
- Technology assets which are within 1 year of the end of their life, or beyond the end of their life, as defined by their manufacturer;
- Technology assets which are unsupported by their manufacturer, or within 2 years of being unsupported;

- Workloads which are and those which are not hosted by a commercial cloud service provider as defined in the NIST publication 500-292; and
- Service level disruptions and their average duration.

State Cybersecurity Act

Agency Cybersecurity

Section 6 amends s. 282.318, F.S., to broaden agency cybersecurity duties, requiring that each state agency head:

- Designate a chief information security officer to integrate the technical and operational cybersecurity efforts at their agency with the Cybersecurity Operations Center (CSOC), or request that the FLDS procure one for them. This chief information security officer will report to the agency's CIO;
- Provide notice of the designation of a chief information security officer to the FLDS by January 1, annually; and
- Incorporate the Florida State Guard resources.

The bill clarifies that the role of the agency information security managers is to ensure agency compliance with cybersecurity governance, manage risk, and ensure compliance with the state's incident response plan.

State agencies must now conduct their comprehensive cybersecurity risk assessments on an annual basis, rather than triennially, per the criteria, methodology, and scope developed by the state CIO. The bill allows the risk assessment to be facilitated by the DMS, or completed by a private sector vendor. The agency head or his or his designee, and the FLDS must sign off on the risk assessment's findings.

Cybersecurity Incident Reporting Requirements

Sections 6 and 7 broaden the FLDS' role in reporting of cybersecurity incidents at agencies and local governments. The bill:

- Grants the FLDS authority to respond to any state agency cybersecurity incident;
- Requires an agency and local government to report any level cybersecurity incident to the FLDS within 4 hours of discovery of the incident; and
- Requires an agency and local governments to report a ransomware incident to the FLDS within 2 hours of its discovery.

The FLDS must notify the Governor, Senate President, and Speaker of the House of Representatives of an agency's or local government's failure to timely report a cybersecurity incident. The CSOC must also notify the Governor, Senate President, and Speaker of the House of Representatives, in a secure environment, of level 3, 4, or 5 cybersecurity incidents.

The bill amends an agency's or local government's duty to report cybersecurity incidents to the DLE's Cybercrime Office and the CSOC, whereas previously, level 1 or 2 incidents were required to be reported *as soon as possible*, now they must report within the timeframes listed above.

Emergency Support Function

The bill clarifies the DMS' (acting through the FLDS) role under the state comprehensive emergency management plan, requiring that it "lead an emergency support function, ESF CYBER *and DIGITAL*." This refers to its responsibility to assist not only with cybersecurity, in accordance with ESF CYBER standards, but also to assist with any digital needs the state may have, such as the creation of a website, during a period of emergency.

Cybersecurity Briefings

The DMS, acting through the FLDS, is also vested with the duty to provide cybersecurity briefings to legislative members of committees or subcommittees that are responsible for cybersecurity policy.

The bill also allows legislative committees or subcommittees that are responsible for cybersecurity-related policy to hold closed meetings for the purpose of briefing the body on records that are confidential and exempt pursuant to s. 282.318(5) and (6), F.S.

Florida Cybersecurity Advisory Council

Section 8 amends s. 282.319, F.S., to remove the requirement that one of the representatives appointed to the Florida Cybersecurity Advisory Council be from a water treatment facility.

Liability for Cybersecurity Incident-Related Torts

Section 9 amends s. 786.401, F.S., to provide that a county or municipality that substantially complies with incident notification requirements in s. 282.3185, F.S., is not liable for torts related to a cybersecurity incident. It further states that a county's or municipality's failure to substantially implement a cybersecurity program that complies with s. 282.3185, F.S., does not constitute evidence of negligence or negligence per se.

The bill establishes the same bar on liability for private businesses[65] that are involved in a cybersecurity incident, if the entity substantially complies with the data breach notice requirements of s. 501.171, F.S., if applicable, and have:

- Adopted a cybersecurity program that substantially aligns with the current version of the:
  - NIST Framework for Improving Critical Infrastructure Cybersecurity;
  - NIST special publication 800-171;
  - NIST special publications 800-53 and 800-53A;
  - Federal Risk and Authorization management Program security assessment framework;
  - CIS Critical Security Controls; or
  - International Organization for Standardization/International Electrotechnical Commission 27000-series family of standards; or
- Substantially conformed its cybersecurity to the following laws, if regulated by state or Federal governments, or is otherwise subject to the requirements of any of the following laws and regulations:

[65] The bill limits this to sole proprietorships, partnerships, corporations, trusts, estates, cooperatives, associations, or other commercial entities. Additionally, it specifically applies to businesses that acquire, maintain, store, or use personal information

- Security requirements of HIPAA;
- Title V of the Gramm-Leach-Bliley Act of 1999;
- Federal Information Security Modernization Act of 2014; or
- Health Information Technology for Economic and Clinical Health Act.

The following factors should be used to determine a private business' or covered entity's substantial compliance with the standards provided in the bill:

- Size and complexity of the covered entity;
- Nature and scope of the covered entity's activities; and
- Sensitivity of the information that the business protects.

A commercial entity that substantially complies with a combination of industry-recognized cybersecurity frameworks or standards, including the payment card industry data security standard, is provided a presumption against liability for a cybersecurity incident only if it updates its compliance with the frameworks or standards outlined in subsection (2) within 1 year of the latest publication date stated in the revision after two or more of its pertinent frameworks or standards have been updated.

Whether the defendant is a local government, private business, or covered entity, it has the burden of proof to establish their substantial compliance to reach the bar on liability.

Lastly, the bill provides that s. 786.401, F.S., does not establish a private cause of action.

Miscellaneous

Section 1 provides that this Act may be entitled the "Florida Cyber Protection Act."

Section 2 amends s. 110.205, F.S., to classify personnel who are employed by or who report to the state chief information security officer, the state chief data officer, a chief information security officer, and an agency information security manager as select exempt personnel, rather than career services.

Section 3 amends definitions used in ch. 282, F.S., to provide and amend definitions for some of the terms introduced by amendments to the bill.

Section 10 provides that the act takes effect on July 1, 2023.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

Not applicable. The mandate restrictions do not apply because the bill does not require counties and municipalities to spend funds, reduce counties' or municipalities' ability to raise revenue, or reduce the percentage of state tax shared with counties and municipalities.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

Open Meetings

Meetings of the Legislature must be open and noticed as provided in article. III, section 4(e), of the Florida Constitution, except with respect to those meetings exempted by the Legislature pursuant to article I, section 24, Florida Constitution, or specifically closed by the Constitution.[66] The Legislature must adopt rules which provide that all legislative committee and subcommittee meetings of each house and joint conference committee meetings be open and noticed.[67] Such rules must also provide:

> [A]ll prearranged gatherings, between more than two members of the legislature, or between the governor, the president of the senate, or the speaker of the house of representatives, the purpose of which is to agree upon formal legislative action that will be taken at a subsequent time, or at which formal legislative action is taken, regarding pending legislation or amendments, shall be reasonably open to the public. All open meetings shall be subject to order and decorum. This section shall be implemented and defined by the rules of each house, and such rules shall control admission to the floor of each legislative chamber and may, where reasonably necessary for security purposes or to protect a witness appearing before a committee, provide for the closure of committee meetings. Each house shall be the sole judge for the interpretation, implementation, and enforcement of this section.

Rule 1.44 of the Florida Senate requires that all meetings at which legislative business[68] is discussed between two or more members of the Legislature be open to the public, unless, at the sole discretion of the President after consultation with appropriate authorities—the meeting concerns measures to address security, espionage, sabotage, attack, and other acts of terrorism, or for the protection of a witness as required by law.

Lines 1045 through 1051 of the bill state that legislative committees or subcommittees that are responsible for matters that relate to cybersecurity may hold closed meetings

[66] FLA. CONST. art. I, s. 24.
[67] FLA. CONST. art. III, s. 4(e).
[68] "Legislative business" is defined as "issues pending before, or upon which foreseeable action is reasonably expected to be taken by the Senate, a Senate committee, or a Senate subcommittee." Fla. Senate R. 1.44.

closed, if approved by the respective legislative body under the rules of such legislative body. This is duplicative of Senate Rule 1.44. Additionally, it may conflict with article III, section 4(e), of the Florida Constitution, because the statute—rather than a legislative rule or constitutional provision—provides for the methods in which a Legislative body may close its meetings.

Lines 352-378 create an operations committee that will consist of the CIO and many state agency heads, or their designees. This may present a need to notice a public meeting whenever the CIO discusses cybersecurity issues with any other member of the operations committee—whether or not it is for operations committee business.[69] This may cause issues in the performance of some of the CIO's assigned duties regarding oversight of agency cybersecurity operations.

Access to Courts

The State Constitution provides in Article 1, s. 21, that "[the courts shall be open to every person for redress of any injury, and justice shall be administered without sale, denial or delay."

Case law has demonstrated, however, that this provision is not absolute. In 1973, the Florida Supreme Court, in *Kluger v. White*,[70] held that it would not completely prohibit the Legislature from altering a cause of action, but would not allow it to "destroy a traditional and long-standing cause of action upon mere legislative whim…"

The case involved the abolition of a statute governing a tort action for property damage in an automobile accident case. When the Legislature abolished the remedy, it did not provide an alternative protection to the injured party. The Court was confronted with the issue of whether the Legislature could abolish a right of access to the courts. The Court determined that the Legislature may not abolish a pre-1968 common law right or a statutory cause of action unless the Legislature provides a reasonable alternative to that action or unless an overpowering public necessity exists for abolishing the right of action. The Court applies a three-part test to determine whether a statute violates the access to courts provision:

- Does the change abolish a preexisting right of access?
- If so, whether a reasonable alternative exists to protect that preexisting right of access.
- If no reasonable alternative exists, whether an overwhelming public necessity exists.[71]

Restrictions on the ability to bring a lawsuit have been upheld as constitutional, but the point at which a restriction becomes an unconstitutional bar is not well defined.

Impairment of Contracts

The bill unilaterally transfers a contract with a private party to a new government entity. The United States Constitution and the Florida Constitution prohibit the state from

[69] *See, e.g., Florida Citizens Alliance, Inc. v. School Board of Collier County*, 328 So.3d 22 (Fla. 2d DCA 2021).
[70] *Kluger v. White*, 281 So. 2d 1 (Fla. 1973).
[71] *Eller v. Shova*, 630 So. 2d 537 (Fla. 1993).

passing any law impairing the obligation of contracts.[72] "[T]he first inquiry must be whether the state law has, in fact, operated as a substantial impairment of a contractual relationship. The severity of the impairment measures the height of the hurdle the state legislation must clear."[73] If a law does impair contracts, the courts will assess whether the law is deemed reasonable and necessary to serve an important public purpose.[74] The factors that a court will consider when balancing the impairment of contracts with the public purpose include:

- Whether the law was enacted to deal with a broad, generalized economic or social problem;
- Whether the law operates in an area that was already subject to state regulation at the time the parties undertook their contractual obligations, or whether it invades an area never before subject to regulation; and
- Whether the law results in a temporary alteration of the contractual relationships of those within its scope, or whether it permanently and immediately changes those contractual relationships, irrevocably and retroactively.[75]

It is unclear to what extent the provisions specific to the state data center and the Northwest Regional Data Center contract will be impaired as a result of this bill. The requirement that the state data center fully integrate with the cybersecurity operations center could at least require an amendment to the current contract.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

Private businesses may enjoy lower cyber liability insurance premiums as a result of their shield from liability created by the bill.

C. Government Sector Impact:

The bill may increase state expenditures related to cybersecurity oversight.

VI. Technical Deficiencies:

The committee created on lines 282-311 of the bill is an advisory body adjunct to an executive agency, and therefore must be established and maintained in accordance with the requirements of s. 20.052, F.S. The committee must be created pursuant to a finding of necessity and public benefit, and be terminated when it no longer serves that purpose. Additionally, meetings of any

[72]U.S. Const. Article I, s. 10; Art. I, s. 10, Fla. Const.
[73]*Pomponio v Claridge of Pompano Condominium, Inc.*, 378 So. 2d 774, 779 (Fla. 1979) (quoting *Allied Structural Steel Co. v. Spannaus*, 438 U.S. 234, 244-45 (1978)). *See also General Motors Corp. v. Romein*, 503 U.S. 181 (1992).
[74]*Park Benziger & Co. v. Southern Wine & Spirits, Inc.*, 391 So. 2d 681, 683 (Fla. 1980); *Yellow Cab Co. of Dade County v. Dade County*, 412 So. 2d 395, 397 (Fla. 3rd DCA 1982) (citing *United States Trust Co. v. New Jersey*, 431 U.S. 1 (1977)).
[75]*See supra* note 2.

collegial body created by specific statutory enactment as an adjunct to an executive agency must be open to the public, in accordance with s. 286.011, F.S., and minutes must be maintained.

VII. Related Issues:

Legislative Briefing on Confidential and Exempt Subject Matter
The bill's provision that allows any legislative committee or subcommittee that is responsible for cybersecurity-related issues to hold closed meetings for the purposes of being briefed on confidential and exempt subject matter is duplicative of the Legislature's current ability to do so.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 282.0041, 282.0051, 282.201, 282.318, 282.3185, and 282.319.

This bill creates section 768.401of 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 by Governmental Oversight and Accountability on March 29, 2023:
The committee substitute:

- Classifies personnel employed by or reporting to the state CISO, state chief data officer, a chief information security officer, and an agency information security manager as select exempt.
- Removes language in the bill that would have shifted authority relating to cybersecurity governance from the DMS to the FLDS.
- Provides DMS additional IT project and cybersecurity incident monitoring oversight.
- Modifies the FLDS' operations committee's membership.
- Requires the CIO to designate a state chief technology officer, and outlines its duties.
- Restores the $10 million threshold for the FLDS' oversight of agency IT projects.
- Specifies oversight of the State Data Center and requires the FLDS rather than the DMS to appoint its director.
- Requires the SDC to fully integrate with the CSOC.
- Requires state agencies to designate a chief information technology security officer, in addition to their information security manager. This new position will integrate the agency's technical and operational cybersecurity efforts with the CSOC.
- Requires agencies to conduct their comprehensive risk assessment annually, rather than triennially, and requires that it be conducted in accordance with criteria developed by the CISO.
- Removes language that required legislative members to be invited to the Cybersecurity Advisory Council Meetings.
- Removes language that created the State Technology Advancement Council.

- Clarifies that a local government or private business that seeks the protection from liability created by the bill has the burden to prove substantial compliance with specific cybersecurity protocols.

B. Amendments:

None.