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:	SB 1662
INTRODUCER:	Senator Collins
SUBJECT:	Cybersecurity
DATE:	January 26, 2024
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Harmsen	McVaney	GO	**Pre-meeting**
2.			AEG	
3.			AP	

I. Summary:

Over the last decade, cybersecurity has rapidly become a growing concern. Currently, the Department of Management Services (DMS) oversees information technology (IT) governance and security for the executive branch of state government. Through the Florida Digital Service (FLDS), the DMS implements duties and policies for IT and cybersecurity for state agencies.

SB 1662:

- Expands the FLDS' duties;
- Provides that the state chief information officer (CIO), in consultation with the Secretary of DMS, must designate a state chief technology officer and specifies the position's responsibilities;
- Requires the FLDS to create guidelines for and ensure independent project oversight on all state agency IT projects of $25 million or more (up from $10 million in current law);
- Deletes the requirement that the FLDS conduct annual assessments of state agencies to determine compliance with the DMS' IT standards and guidelines;
- Requires state agencies to designate a chief information security officer to integrate the agency's technical and operational cybersecurity efforts with Cybersecurity Operations Center (CSOC). These CISOs will be administratively housed within the individual agency, but will report to the state CIO within the FLDS;
- Shortens the timeframe in which state agencies must report ransomware and cybersecurity incidents, and applies this notification requirement to all such incidents, regardless of severity level;
- Removes the Florida Department of Law Enforcement's (FDLE) Cybercrime Office from the parties that must receive immediate notification of ransomware and cybersecurity incidents, instead requiring notification to the only the DMS' CSOC. The CSOC must then immediately notify the FDLE cybercrime office of such notifications from state agencies, and the Cybercrime Office and the local sheriff for notifications from local governments;

- Requires CSOC to immediately notify the state CIO and the state cyber security information officer of a reported incident;
- Classifies certain IT security personnel as selected exempt, allowing the DMS to set their benefits and pay within applicable rules;
- Authorizes the DMS to brief legislative committees that are responsible for cybersecurity policy on cybersecurity matters in a closed setting;
- Allows a legislator who serves on a committee that is responsible for cybersecurity policy to attend Cybersecurity Advisory Council (CAC) meetings, including those portions that are closed to the Sunshine;
- Permits the DMS to exercise authority to obtain immediate access to public or private infrastructure that hosts agency data, and to direct measures to assess, monitor, and safeguard that data; and
- Requires that one of the three representatives on the CAC from the critical infrastructure sectors must be from a utility provider and requires that one of the members of the CAC is a representative from a local government.

The bill may increase state expenditures relating to new positions within and duties assigned to the FLDS and the DMS, and to additional authorities assigned to the FLDS.

The bill provides an effective date of July 1, 2024.

II. Present Situation:

Over the last decade, cybersecurity has rapidly become a growing concern. The cyberattacks are growing in frequency and severity. Cybercrime is expected to inflict $8 trillion worth of damage globally in 2023.[1] The United States is often a target of cyberattacks,[2] including attacks on critical infrastructure, and has been a target of more significant cyberattacks[3] over the last 14 years than any other country.[4] The Colonial Pipeline is an example of critical infrastructure that was attacked, disrupting what is arguably the nation's most important fuel conduit.[5]

Ransomware is a type of cybersecurity incident where malware[6] that is designed to encrypt files on a device and renders the files and the systems that rely on them unusable. In other words,

---

[1] Steve Morgan, CYBERCRIME MAGAZINE, *Cybercrime to Cost the World $8 Trillion Annually in 2023* (Oct, 17, 2022), Cybercrime To Cost The World 8 Trillion Annually In 2023 (cybersecurityventures.com) (last visited Jan. 25, 2024).
[2] Chris Jaikaran, CONGRESSIONAL RESEARCH SERVICE, *Cybersecurity: Selected Cyberattacks, 2012-2022* (Aug. 9, 2023), https://crsreports.congress.gov/product/pdf/R/R46974 (last visited Jan. 25, 2024).
[3] "Significant cyber-attacks" are defined as cyber-attacks on a country's government agencies, defense and high-tech companies, or economic crimes with losses equating to more than a million dollars. Kyle Brasseur, FRA CONFERENCES, *Study: U.S. Largest Target for Significant Cyber-Attacks* (Jul. 13, 2020), https://www.fraconferences.com/insights-articles/compliance/study-us-largest-target-for-significant-cyber-attacks/#:~:text=The%20United%20States%20has%20been%20on%20the%20receiving,article%20is%20from%20FRA%27s%20sister%20company%2C%20Compliance%20Week (last visited March 21, 2023).
[4] *Id*.
[5] S&P Global, *Pipeline operators must start reporting cyberattacks to government: TSA orders*, https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/electric-power/052721-pipeline-operators-must-start-reporting-cyberattacks-to-government-tsa-orders?utm_campaign=corporatepro&utm_medium=contentdigest&utm_source=esgmay2021 (last visited Jan. 25, 2024).
[6] "Malware" means hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. malware - Glossary | CSRC (nist.gov) (last visited Jan. 25, 2024).

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.[7] 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.[8]

Information Technology and Cybersecurity Management

The Department of Management Services (DMS) oversees information technology (IT)[9] governance and security for the executive branch in Florida.[10] The Florida Digital Service (FLDS) is housed within the DMS and was established in 2020 to replace the Division of State Technology.[11] The FLDS works under the DMS to implement policies for information technology (IT) and cybersecurity for state agencies.[12]

The head of the FLDS is appointed by the Secretary of Management Services[13] and serves as the state chief information officer (CIO).[14] 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.[15] 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.[16]

The DMS, through the FLDS, has the following powers, duties, and functions:[17]

- Develop IT policy for the management of the state's IT resources;

---

[7] Cybersecurity and Infrastructure Agency, *Ransomware 101*, https://www.cisa.gov/stopransomware/ransomware-101 (last visited March 21, 2023).
[8] Caitlyn Stroh-Page, TALLAHASSEE DEMOCRAT, *Social Security Numbers, Some Patient Treatment Info Involved in TMH Cybersecurity Incident* (Apr. 1, 2023) https://www.tallahassee.com/story/news/local/2023/03/31/tmh-updates-what-information-was-affected-during-cybersecurity-incident/70069655007/ (last visited Jan. 25, 2024).
[9] 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(19), F.S.
[10] *See* s. 20.22, F.S.
[11] Chapter 2020-161, Laws of Fla.
[12] *See* s. 20.22(2)(b), F.S.
[13] 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.
[14] Section 282.0051(2)(a), F.S.
[15] *Id*.
[16] Section 282.0051(1), F.S.
[17] *Id*.

- Develop an enterprise architecture;
- Establish IT project management and oversight standards for state agencies;
- Oversee 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;[18] and
- Standardize and consolidate IT services that support interoperability, Florida's cloud first policy, and business functions and operations that are common across state agencies.

State Cybersecurity Act

While it has existed in some form for more than 10 years, in 2022, the Legislature passed the State Cybersecurity Act,[19] which requires the DMS and the heads of the state agencies[20] to meet certain requirements to enhance the cybersecurity[21] of the state agencies.

The DMS through FLDS is tasked with completing the following:[22]

- Establish standards for assessing agency cybersecurity risks;
- Adopt rules to mitigate risk, support a security governance framework, and safeguard agency digital assets, data,[23] information, and IT resources;[24]
- Designate a chief information security officer (CISO);
- Develop and annually update a statewide cybersecurity strategic plan such as identification and mitigation of risk, protections against threats, and tactical risk detection for cyber incidents;[25]
- Develop and publish for use by state agencies a cybersecurity governance framework;
- Assist the state agencies in complying with the State Cybersecurity Act;
- Provide annual training on cybersecurity for information security managers and computer security incident response team members;
- Annually review the strategic and operational cybersecurity plans of state agencies;
- Track the state agencies' implementation of remediation plans;
- Provide cybersecurity training to all state agency technology professionals that develops, assesses, and documents competencies by role and skill level;

[18] 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.
[19] Section 282.318, F.S.
[20] 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.
[21] "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.
[22] Section 282.318(3), F.S.
[23] "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.
[24] "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.
[25] "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.

- Maintain 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
- Lead an Emergency Support Function under the state emergency management plan.

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.[26] The head of the agency has additional tasks in protecting against cybersecurity threats as follows:[27]

- Establish a cybersecurity incident response team with the FLDS and the Cybercrime Office, which must immediately report all confirmed or suspected incidents to the CISO;
- Annually submit to the DMS the state agency's strategic and operational cybersecurity plans;
- Conduct and update a comprehensive risk assessment to determine the security threats once every three years;
- Develop and update written internal policies and procedures for reporting cyber incidents;
- Implement safeguards and risk assessment remediation plans to address identified risks;
- Ensure internal audits and evaluations of the agency's cybersecurity program are conducted;
- Ensure that the cybersecurity requirements for the solicitation, contracts, and service-level agreement of IT and IT resources meet or exceed applicable state and federal laws, regulations, and standards for cybersecurity, including the National Institute of Standards and Technology (NIST)[28] cybersecurity framework;
- Provide cybersecurity training to all agency employees within 30 days of employment;
- Develop a process that is consistent with the rules and guidelines established by the FLDS for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents; and
- Submit an after-action report to the FLDS within one week after remediation of a cybersecurity incident or ransomware incident.

Florida Cybersecurity Advisory Council

The Florida Cybersecurity Advisory Council[29] (CAC) within the DMS[30] assists state agencies in protecting IT resources from cyber threats and incidents.[31] The CAC must assist the FLDS in implementing best cybersecurity practices, taking into consideration the final recommendations of the Florida Cybersecurity Task Force – a task force created to review and assess the state's cybersecurity infrastructure, governance, and operations.[32] The CAC meets at least quarterly to:[33]

- Review existing state agency cybersecurity policies;

[26] Section 282.318(4)(a), F.S.
[27] Section 282.318(4), F.S.
[28] NIST, otherwise known as the National Institute of Standards and Technology, "is a non-regulatory government agency that develops technology, metrics, and standards to drive innovation and economic competitiveness at U.S.-based organizations in the science and technology industry." Nate Lord, *What is NIST Compliance*, DataInsider (May. 6, 2023), https://www.digitalguardian.com/blog/what-nist-compliance (last visited Jan. 25, 2024).
[29] 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.
[30] Section 282.319(1), F.S.
[31] Section 282.319(2), F.S.
[32] Section 282.319(2)-(3), F.S.
[33] Section 282.319(9), F.S.

- 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; and
- Examine inconsistencies between state and federal law regarding cybersecurity.

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.[34]

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 as stated below:[35]

- 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.

Cyber Incident Response

The National Cyber Incident Response Plan (NCIRP) was developed by the U.S. Department of Homeland Security, according to the direction of Presidential Policy Directive (PPD)-41.[36] The NCIRP is part of the broader National Preparedness System and establishes the strategic framework for a whole-of-Nation approach to mitigating, responding to, and recovering from cybersecurity incidents posing risk to critical infrastructure.[37] 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

[34] Section 282.319(10), F.S.
[35] Section 282.319(11), F.S.
[36] Annex for PPD-41: *U.S. Cyber Incident Coordination*, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident (last visited Jan. 25, 2024).
[37] Cybersecurity & Infrastructure Security Agency, *Cybersecurity Incident Response*, 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 Jan. 25, 2024).

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.[38]

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.[39]

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 three, four, or five 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.[40] 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 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.[41] For state agency incidents at severity levels one and two, they must report these to the CSOC and the Cybercrime Office at the FDLE as soon as possible.[42]

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; and

[38] *Id.*
[39] Section 282.318(3)(c)9.a, F.S.
[40] Sections 282.318(3)(c)9.c(I), F.S. and 282.3185(5)(b)1., F.S.
[41] Section 282.318(3)(c)9.c.(II), F.S.
[42] Section 282.318(3)(c)(9)(d), F.S.

- If the reporting entity is a local government, a statement requesting or declining assistance from the CSOC, FDLE Cybercrime Office, or sheriff.[43]

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.[44] 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.[45]

State agencies and local governments must submit an after-action report to the FLDS within one week of the remediation of a cybersecurity or ransomware incident.[46] The report must summarize the incident, state the resolution, and 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.[47] 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.[48] Additionally, any document that, when held by an agency, is exempt or confidential and exempt under s. 119.07(1), F.S., maintains its exempt status when the custodian agency shares it with the legislature.[49]

The State Cybersecurity Act also exempts portions of any public meeting that would reveal records that it makes confidential and exempt.[50]

Florida Fusion Center

To help unify the Nation's efforts to share information and exchange intelligence, the Intelligence Reform and Terrorism Prevention Act of 2004 (Act) was passed. The Act provides guidance to agencies at all levels about information sharing, access and collaboration. Part of this guidance is the need to designate a single fusion center in each state to serve as the "hub" for these activities.[51]

[43] Section 282.318(3)(c)9.b, F.S.
[44] Section 282.318(3)(c)9.e, F.S.
[45] *Id.*
[46] Section 282.318(4)(k), F.S.
[47] Section 282.318(5), F.S.
[48] Section 282.318(7), F.S.
[49] Section 11.0431(2)(a), F.S.
[50] Section 282.318(6), F.S.
[51] Florida Department of Law Enforcement, *Florida Fusion Center History*, https://www.fdle.state.fl.us/FFC/FusionCenterHistory (last visited January 25, 2024).

The Florida Fusion Center, also known as FFC, began operations in 2007 and is located in Tallahassee, Florida. The FFC was designated as the state's primary fusion center by the Governor in March of 2008 and serves as the head of the Network of Florida Fusion Centers. There are regional fusion centers in each of the seven FDLE regions to support local and state intelligence needs. [52]

The FFC provides connectivity and coordinates intelligence sharing among seven regional fusion centers located throughout the state. Operations are guided by the understanding that the key to effectiveness is the development and sharing of information to the fullest extent permitted by law and agency policy. The FFC consists of approximately 45 FDLE members, federal agencies, and twelve multi-disciplinary state agency partners; and includes outreach to private sector entities.[53]

III. Effect of Proposed Changes:

Section 1 classifies as selected exempt service[54] chief information security officers, information security managers that are designated by s. 282.318(4), F.S., and personnel who are employed by or report to the state CISO, the state chief data officer, or an agency information security manager; some of these personnel would otherwise be classified as career service. The DMS must establish the salary and benefits for agency information security managers in accordance with Senior Management Service Rules, and for the remaining categories in accordance with the rules of the Selected Exempt Service, unless the salary and benefits are otherwise fixed by law.

IT Project Oversight

Section 3 expands the FLDS' powers, duties, and functions, vesting it with the authority to:

- Lead enterprise cybersecurity efforts;
- Safeguard enterprise digital data; and
- Test, develop, and deploy solutions that securely modernize state government, including technology and information services.

The bill amends the FLDS' duty to perform project oversight of state IT projects and create related guidelines to require the FLDS to "ensure that independent project oversight…is performed in compliance with applicable state and federal law." This will apply to state agency IT projects that will cost $25 million or more, rather than $10 million.

The bill maintains the FLDS' duty to perform project oversight, rather than ensure, on IT projects for the DFS, DLA, and DACS, but increases the total project cost which qualifies the IT project for FLDS oversight from $20 million to $25 million.

[52] *Id*.
[53] Florida Department of Law Enforcement, *Long-Range Program Plan Fiscal Years 2010-2011 through 2014-2015, September 30, 2009*, available at http://floridafiscalportal.state.fl.us/Document.aspx?ID=2215&DocType=PDF (last visited Jan. 25, 2024).
[54] The Selected Exempt Service is a separate system of personnel administration for specified positions in state government. Section 110.602, F.S.

The bill designates a new office within the FLDS, the state chief technology officer, who will supervise the creation of IT project standards and related project oversight. Additionally, the bill increases the threshold at which state agencies must allow for pre-contract IT project oversight and input from the FLDS from $10 million to $25 million.

Section 3 deletes the FLDS' duty to annually assess and report on state agency compliance with IT standards and guidelines, as developed by the DMS.

State Chief Technology Officer

Section 3 also creates the position of state chief technology officer, who is responsible for:
- Establishing and maintaining an enterprise architecture framework that ensures that IT investments align with Florida's strategic objectives and initiatives;
- Conducting comprehensive evaluations of potential technological solutions;
- Cultivating strategic partnerships among both the state enterprise agencies and the private sector to develop expertise, promote collaboration, and advance Florida's technological capabilities;
- Supervising program management of specific state agency IT projects;
- Providing advisory support and oversight for technology-related projects; and
- Identifying and recommending best practices to enhance the state's technological efficiency and effectiveness, and technology project outcomes.

The CIO, in consultation with the Secretary of DMS, will designate the state chief technology officer.

Enterprise Digital Data

Section 3 amends s. 282.0051(5), F.S., to delete the requirement that the DMS enter into a shared-data agreement with an agency that has primary custody responsibility of, or data-sharing responsibility for, data before the DMS may retrieve or disclose such data.

The bill defines "enterprise digital data" as information that is held by a state agency in electronic form that is deemed to be owned by the state and held for state purposes by the state agency. It further states that enterprise digital data that is subject to statutory requirements for particular types of sensitive data or to contractual limitations for data marked as trade secrets or sensitive corporate data held by state agencies "shall be treated in accordance with such requirements or limitations" and that the DMS must maintain personnel who are appropriately certified to "steward such enterprise digital data" and must also be maintained in accordance with chapter 119, F.S.

It is unclear how an agency that agrees to be the sole custodian of such data may comply with such contractual provisions if the agency is also required to share the data with the FLDS. Similarly, certain public records exemptions apply only when held by the specific custodian agency; the exemption does not necessarily transfer with the record if it is disclosed to a different agency.

Cybersecurity

Section 5 amends s. 282.318, F.S., to make FLDS the sole entity responsible for leading cybersecurity efforts and safeguarding agency digital data, in addition to the current duties of establishing standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures. The DMS "acting through the FLDS" was formerly responsible for this provision.

Cybersecurity Operations Center

Agency Notifications to CSOC

Pursuant to s. 282.318(3)(c)9.c.(I), F.S., state agencies must report all ransomware incidents and any cybersecurity incidents of severity levels 3-5 to the CSOC and the FDLE Cybercrime Office within specific timeframes. The bill narrows this reporting requirement, requiring an agency to report only to the CSOC, not to the FDLE. However, the agency must now report *all* ransomware incidents and cybersecurity incidents, regardless of their severity level, and must do so no later than 12 hours (for cybersecurity incidents) or 6 hours (for ransomware incidents) after discovery of the incident.

After such a notification, the CSOC must immediately notify the FDLE Cybercrime Office and provide regular reports on the incident's status, preserve forensic data; and provide aid to the Cybercrime's investigate efforts; if the CISO finds that such efforts do not impede remediation of the incident and that there is no risk to the public or to critical state functions. The CSOC must also immediately notify the CIO and CISO of any ransomware or cybersecurity incident reported by an agency. Within 24 hours of receipt of such information, the CISO, rather than the CSOC, must notify within a secure environment the President of the Senate and Speaker of the House of Representatives of incidents with a severity level of 3-5.

Similarly, the bill amends s. 282.318(3)(a), F.S., to require the CSOC to immediately notify the CIO and CISO of all confirmed or suspected incidents or threats to state agency IT resources.

Local Government Notifications to CSOC

The bill removes the requirement that a local government must report any cybersecurity incident determined to be level 3, 4, or 5 to the Cybercrime Office of FDLE and the sheriff who has jurisdiction over the local government. The bill instead requires a local government to report a cybersecurity incident to CSOC within 12 hours of discovery and to report a ransomware incident within 6 hours after discovery.

After CSOC receives such a report from a local government, the CSOC must immediately notify the FDLE Cybercrime Office and the local sheriff with jurisdiction over the local government. The CSOC must provide these entities with regular reports on the status of the incident, preserve forensic data to support a subsequent investigation, and provide aid to the investigative efforts of the Cybercrime Office upon the office's request if the state CISO finds that the investigation does not impede remediation of the incident and that there is no risk to the public and no risk to critical state functions.

Similarly, the bill requires the CSOC to immediately notify the CISO of the reported incident. The state CISO must notify the President of the Senate and the Speaker of the House of

Representatives in a secure environment, no later than 24 hours after receiving report of the incident.

A local government is permitted, but not required, to report a level 1 or 2 cybersecurity incident to the CSOC. If the CSOC receives this optional report, it must conduct the same notifications and reporting as is required for a local government's report of a level 3-5 cybersecurity incident.

Quarterly Incident Reports from CSOC
The CSOC must now additionally distribute its quarterly consolidated incident report to the Governor, Attorney General, and executive director of the FDLE, in addition to the President of the Senate, Speaker of the House of Representatives, and Cybersecurity Advisory Council.

Cybersecurity Briefings

The bill requires the DMS, through the FLDS, to provide cybersecurity briefings to the members of any legislative committee or subcommittee that is responsible for policy matters that relate to cybersecurity.

Section 282.318(10), F.S. is amended to allow 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), F.S. The bill directs that such meetings must be closed by the respective body pursuant to its rules, if the briefing includes records made confidential and exempt pursuant to s. 282.318(5) and (6), F.S., which includes portions of risk assessments, evaluations, external audits, and other agency cybersecurity reports; and state agency IT resources.[55] This may be duplicative of the duty to provide briefings found on lines 598-600. The bill also provides that a legislative committee or subcommittee must maintain the confidential and exempt status of such records. This is duplicative of s. 11.0431, F.S., which requires the Legislature to maintain exempt or confidential and exempt records in the same manner required by the agency.

Cybersecurity Advisory Council

Section 7 amends s. 282.319, F.S., to amend the membership requirements of the Advisory Council. The bill replaces the requirement that the Governor appoint a water treatment facility representative as one of the three representatives from critical infrastructure sectors, with a requirement that one of the members be a representative of a utility provider. The bill also adds a representative of local government to the Council's overall required membership.

The bill states that legislative members of legislative committees or subcommittees that are responsible for cybersecurity policy must be invited to attend Advisory Council meetings, including any portion closed to the public pursuant to s. 286.011 and s. 24(b), Art. I of the State Constitution.

[55] Section 282.318(6), F.S., makes exempt from public meetings laws any portion of a meeting that would reveal documents that are confidential and exempt under s. 282.318(5), F.S.

Access to Infrastructure

Additionally, the bill grants the DMS, through the FLDS, authority to obtain immediate access to public or private infrastructure that hosts enterprise digital data. The bill additionally grants authority to the DMS to direct, in consultation with the state agency that holds the particular enterprise digital data, measures to assess, monitor, and safeguard the digital data.

Agency Chief Information Security Officer

The bill requires each agency head to annually designate, in writing to the FLDS, a chief information security officer to integrate the agency's technical and operational cybersecurity efforts with the CSOC. An agency may request that the DMS procure "as a service" a CISO on its behalf via contracting with or outsourcing to a third party ("as a service," is defined in section 2 as third party contracting or outsourcing.)

The agency CISO, at agencies[56] that are under the Governor's jurisdiction, will be under the general supervision of the agency head or designee for administrative purposes only, but will report to the CISO.

While section 5 of the bill amends s. 282.318(4), F.S., to require only state agency heads (which excludes Cabinet-level agencies by virtue of the definition of "state agency") to designate a CISO, the subsequent language that refers to a "state agency that is under the jurisdiction of the Governor…" Canons of statutory interpretation hold that "courts must give "significance and effect ... to every word, phrase, sentence, and part of the statute if possible, and words in a statute should not be construed as mere surplusage."[57] Therefore, it is unclear whether the general requirement to appoint a state agency CISO applies to all agencies, including Cabinet-level agencies.

Miscellaneous

Section 2 defines terms used in ch. 282, F.S.

The bill updates reporting deadlines throughout to reflect a 15-30 day grace period after the calendar-year or quarterly reporting timeframe.

The bill updates a reference from "ESF CYBER" to "ESF 20"[58] to reflect the current Emergency Support Function for cybersecurity emergency needs, developed as part of the state comprehensive emergency management plan, pursuant to s. 252.35, F.S.

---

[56] Section 282.318(2), defines "state agency" as 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. As used in part I of this chapter, except as otherwise specifically provided, the term does not include the Department of Legal Affairs, the Department of Agriculture and Consumer Services, or the Department of Financial Services.

[57] Raymond James Fin. Servs., Inc. v. Phillips, 126 So. 3d 186 (Fla. 2013), quoting *Hechtman v. Nations Title Ins. of N.Y.*, 840 So.2d 993, 996 (Fla. 2003).

[58] Florida Department of Emergency Management, *Emergency Support Function 20- Cybersecurity Annex* (2022), https://portal.floridadisaster.org/preparedness/External/CEMP/2022%20State%20CEMP%20ESF%2020%20Annex.pdf (last visited Jan. 24, 2024).

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:

Section 3 deletes the current requirement in s. 282.0051(5), F.S., that the DMS retrieve or disclose data only pursuant to a shared-data agreement with the agency that holds the subject data. Additionally, the bill contemplates FLDS' handling of "enterprise digital data" (defined as all state data, which includes public records or documents that are exempt from disclosure as a public record). Although the bill directs that "enterprise digital data must be maintained in accordance with chapter 119", it is unclear that this will achieve the full statutory pubic records exemption protections. Public records law exists throughout the Florida statutes and Constitution, not just in ch. 119, F.S.

Additionally, the act of locating or transferring data outside the originating agency may undermine the document's status as an exempt public record. It may also complicate the individual's duty to provide access to a public record if it is unable to access or organize its stored documents according to its known process.

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.[59] 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.[60] 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

[59] FLA. CONST. art. I, s. 24.
[60] FLA. CONST. art. III, s. 4(e).

> 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[61] 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 598-600 allows the DMS to provide cybersecurity briefings to legislative committees or subcommittees responsible for matters relating to cybersecurity. Additionally, lines 627 through 638 state that legislative committees or subcommittees that are responsible for matters that relate to cybersecurity may hold closed meetings, 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.

Legislative Authority to Review State Agencies

The bill's provision of DMS' authority to provide briefings to specific legislative committees is unnecessary. Senate Rule 2.2 allows any permanent standing committee and standing subcommittee to "maintain a continuous review of the work of the state agencies concerned with their subject areas and the performance of the functions of government within each subject area" and to "invite public officials [and] employees … to appear before the committee or subcommittee to submit information." The committees may also inspect and investigate the records, data, operation, and other related items of any state public agency. The chair of each standing committee and subcommittee may to issue subpoenas, subpoenas *duces tecum*, and other necessary process to compel the attendance of witnesses and the production of evidence.

Access to Private Infrastructure, Unreasonable Search and Seizure

Lines 601-605 grant the DMS, acting through the FLDS, authority to obtain access to public or private infrastructure that hosts enterprise digital data. This appears to allow government access to private property without any basis. This may violate the Fourth Amendment of the U.S. Constitution, which holds that individual privacy and security

[61] "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.

must be safeguarded against arbitrary invasions by governmental officials.[62] "[S]earches conducted outside the judicial process ... are *per se* unreasonable under the Fourth Amendment—subject only to a few ... exceptions."[63] One exception is for administrative searches.[64] To be constitutional, the subject of an administrative search must, among other things, be afforded an opportunity to obtain precompliance review before a neutral decisionmaker.[65] This rule "applies to commercial premises as well as to homes."[66]

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

Private sector IT and cybersecurity companies may have new opportunities to contract with the DMS in its implementation of provisions of the bill.

A private entity with a contract with an individual agency for the storage or other function related to agency data may incur legal fees relating to the attempted renegotiation of its ongoing contract.

C. Government Sector Impact:

The bill will likely have a significant fiscal impact on state agency resources used to employ new positions created by the bill, fund certain positions at higher salary and benefit levels as prescribed by the bill, and implement new guidelines and trainings as required to transfer data ownership and related cybersecurity processes.

There will likely be a transition of public records requests functions to the DMS as it takes on its new role regarding enterprise data, and this could impact the DMS' need for additional staff and trainings and certifications required to respond to such requests and handle specialized data in the manner required by federal law.

Individual agencies and the DMS may be subject to higher litigation fees for the resolution of public records exemption disputes that arise from the new framework of state agency data sharing implemented by the bill.

VI. Technical Deficiencies:

Line 381 requires the DLA, DFS, and DACS to adopt, by rule, standards that facilitate the deployment of applications or solutions to the existing enterprise system in a controlled and phased approach. It is not clear that this constitutes sufficient rulemaking authority for those

[62] *Camara v. Mun. Ct. of City & Cnty. of San Francisco*, 387, U.S. 523, 528 (1967).
[63] *Arizona v. Gant*, 556 U.S. 332, 338 (2009).
[64] *See, Camara v. Municipal Court of City and County of San Francisco,* 387 U.S. 523, 534.
[65] See *See v. Seattle*, 387 U.S. 541, 545.
[66] *Marshall v. Barlow's, Inc.*, 436 U.S. 307, 312 (1978).

agencies to adopt rules; the rulemaking authority may need to be placed in sections of law specific to their agency authority.

Line 418 refers to "threats *of* state agency information technology." It may intend to refer to "threats *to* state agency information technology."

It is not clear when or who must assess the severity level of a cybersecurity incident that occurs at a state agency. The bill deletes the state agency requirement to perform this assessment (see lines 503-504), but, then still requires certain actions based on the severity level determination (see line 527).

The bill requires the CISO to notify the President of the Senate and Speaker of the House of Representatives of certain cybersecurity and ransomware incidents in a "secure environment." This is an undefined term that can be a term of art in both technological and security realms, and it is therefore unclear what standards the bill requires. The agency's or local government's initial report of the cybersecurity or ransomware incidents is not required to be made in a secure environment—it may be unnecessary to require a higher standard of security at a subsequent reporting.

VII. Related Issues:

The bill changes the FLDS' role from the creation of standards and oversight of the implementation of those standards to operation of IT and cybersecurity efforts. It is unclear what functions are included in this role, and it may need to be more clearly defined. For example, it is unclear:

- What enterprise security "efforts" the FLDS must lead (lines 131-132);
- How the DMS, through the FLDS, will "ensure" independent project oversight of agency IT projects (lines 171-172); and
- What a cultivation of strategic partnerships with the private sector to leverage expertise, foster collaboration, and advance Florida's technological capabilities would entail (lines 345-350).

The bill also grants the FLDS supervising program management authority over enterprise IT initiatives, whereas its current authority is to *participate* in such initiatives with the agency (see lines 351-367). The sponsor may wish to more clearly delineate the functions that are required of the FLDS in its supervisory authority.

<u>Enterprise Digital Data, Impairment of Contracts</u>

Through its definition of the term "enterprise digital data," the bill allows the DMS, acting through the FLDS, to take an ownership interest in data that belongs to other agencies. This includes the duties to assess and monitor the data, and the general duty to safeguard it. Additionally, the bill allows the DMS to "obtain immediate access to public or private infrastructure" that hosts such data. This implicates contracts that are currently in effect between private entities and individual state agencies that may require the data to be held in a specific manner, or to not be shared with any other entity. It is not clear that the DMS would be able to assume the individual agency's current contracting authority.

Article I, section 10 of the Florida Constitution prohibits the state from enacting laws that impair the obligation of contracts. While Florida courts have historically strictly applied this restriction, they have exempted laws when they find there is an overriding public necessity for the state to exercise its police powers.[67] This exception extends to laws that are reasonable and necessary to serve an important public purpose,[68] to include protecting the public's health, safety or welfare.[69] For a statute to offend the constitutional prohibition against impairment of contract, the statute must have the effect of changing substantive rights of the parties to an existing contract. Any retroactive application of a statute affecting substantive contractual rights would be constitutionally suspect.[70]

Enterprise Digital Data, Public Records

This broad 'ownership' of agency data also implicates public record exemptions that apply only when the exempt information is held by a specific agency. Therefore, documents "shared" with the FLDS via its assertion of authority over enterprise digital data may lose their exempt status.

Enterprise Digital Data, Trade Secrets

Section 119.0715, F.S., makes trade secrets[71] that are held by an agency confidential and exempt from public inspection and copying. An agency may disclose a trade secret to an officer or employee of another agency or governmental entity *whose use of the trade secret is within the scope of his or her lawful duties* and responsibilities.[72] It is unclear whether the role of the DMS in safeguarding, monitoring, and measuring to assess enterprise digital data equates to a use of a trade secret within his or her lawful duties and responsibilities. Additionally, it is unclear how the DMS will be made aware of the data's status as a trade secret, as such communication usually occurs with the individual recipient agency at the time the document is transmitted to it.

Enterprise Digital Data, Attorney-Client privilege

Certain agencies, such as the Department of Legal Affairs, hold information in the scope of their role as an attorney. For attorney-client privilege to apply in Florida, a communication between the lawyer and client must have been made during the actual rendition of legal services to the client and be "confidential," meaning "it is not intended to be disclosed to third persons" except as provided in the Florida Evidence Code.[73] This sharing of data with the DMS may violate the attorney's ethical requirement to guard the confidentiality of documentation regarding her representation.[74]

---

[67] *Park Benziger & Co. v. Southern Wine & Spirits, Inc.*, 391 So.2d 681 (Fla. 1980).
[68] *Yellow Cab Co. v. Dade County*, 412 So.2d 395 (Fla. 3rd DCA 1982), petition den. 424 So.2d 764 (Fla. 1982).
[69] *Khoury v Carvel Homes South, Inc*., 403 So.2d 1043 (Fla. 1st DCA 1981), petition den. 412 So.2d 467 (Fla. 1981).
[70] *Tri-Properties, Inc. v. Moonspinner Condominium Association, Inc.*, 447 So.2d 965 (Fla. 1st DCA 1984).
[71] A "trade secret" is information, including a formula, pattern, compilation, program, device, method, technique, or process that: (a) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. See, 688.002(4), F.S.
[72] But compare with s. 252.88, F.S., which prohibits the agency from disclosing a trade secret without a final determination by the EPA's Administrator.
[73] Sections 90.502(1)(c) and (2), F.S.; Deanna Rahming, FLORIDA BAR NEWS, The *Attorney-Client Privilege v. the Confidentiality Rule: A Lawyer's Conundrum in the Use and Application of the Evidence Code v. the Rules of Professional Conduct* (Jun. 20, 2023), https://www.floridabar.org/the-florida-bar-news/the-attorney-client-privilege-v-the-confidentiality-rule-a-lawyers-conundrum-in-the-use-and-application-of-the-evidence-code-v-the-rules-of-professional-conduct/ (last visited Jan. 25, 2024).
[74] Rule 4-1.6, R.Reg. the Fla. Bar.

Enterprise Digital Data, Federal Policy

Certain agencies hold data pursuant to federal agreements. The FDLE cites the removal of the DMS' requirement to enter into a data sharing agreement to access agency data as a possible violation risk of the Health Insurance Portability Accountability Act (HIPAA), FBI Criminal Justice Information Services (CJIS) Security Policy, Family Educational Rights and Privacy Act (FERPA), and other federal law.[75] This may also disrupt agreements to access federal data on the FTC Consumer Sentinel Network, which is limited to federal, state, or local law enforcement.[76] agencies.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 110.205, 282.0041, 282.0051, 282.00515, 282.318, 282.3185, 282.319.

IX. Additional Information:

A. Committee Substitute – Statement of Changes:

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

None.

B. Amendments:

None.

[75] FDLE, *SB 1662 Agency Analysis* (Jan. 12, 2024) (on file with the Committee on Governmental Oversight and Accountability).

[76] Federal Trade Commission, *Consumer Sentinel Network*, https://www.ftc.gov/enforcement/consumer-sentinel-network (last visited Jan. 26, 2024). *See, e.g.*, s. 570.077, F.S., which makes criminal or civil intelligence or investigative information, or any other information held by the Department of Agriculture and Consumer Services as part of a joint or multiagency examination with another state or federal agency, confidential and exempt from s. 119.07(1), F.S., The DACS may only obtain, use, and release the information in accordance with the joint or multiagency agreement, or in furtherance of its official duties and responsibilities.