HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/HB 1511 Cybersecurity
SPONSOR(S): Energy, Communications & Cybersecurity Subcommittee, Giallombardo
TIED BILLS: **IDEN./SIM. BILLS:** SB 1708

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Energy, Communications & Cybersecurity Subcommittee	18 Y, 0 N, As CS	Mortellaro	Keating
2) State Administration & Technology Appropriations Subcommittee			
3) Commerce Committee			

SUMMARY ANALYSIS

Over the last decade, cybersecurity has rapidly become a growing concern. Cyberattacks are growing in frequency and severity. Currently, the Department of Management Services (DMS) oversees information technology (IT) governance and security for the executive branch of state government. The Florida Digital Service (FLDS) is housed within DMS and was established in 2020 to replace the Division of State Technology. Through FLDS, DMS implements duties and policies for information technology and cybersecurity for state agencies.

The bill:

- Provides DMS, acting through FLDS, with additional responsibilities related to ensuring the independence of technology project oversight and responding to state agency cybersecurity incidents;
- Requires DMS, through FLDS, to create an operations committee to foster interagency collaboration;
- Requires the state chief information officer (CIO) to designate a state chief technology officer and outlines the responsibilities of that position;
- Specifies oversight of the state data center (SDC) and provides FLDS authority to appoint its director;
- Specifies information that the SDC must report to DMS and FLDS.
- Requires the state CIO to assume responsibility for the contract between DMS and the Northwest Regional Data Center (NWRDC) and requires NWRDC to provide FLDS with access to information regarding operations of the SDC;
- Requires the SDC to fully integrate with the Cybersecurity Operations Center;
- Requires state agencies and local governments to report all ransomware incidents within 4 hours and all cybersecurity incidents within 2 hours and adds FLDS to the list of entities to receive such reports;
- Provides new requirements for heads of state agencies related to cybersecurity;
- Creates a career service exemption for particular positions;
- Requires FLDS to provide cybersecurity briefings to members of specified legislative committees;
- Provides that specified legislative committees may hold meetings closed by the respective legislative body when being briefed on certain information; and
- Provides that a government or private entity is not liable for events connected to a cybersecurity incident if it meets specified standards.

The bill does not have a fiscal impact on state or local government revenues or local government expenditures. The bill may increase state expenditures. *See* Fiscal Analysis & Economic Impact Statement.

The bill provides an effective date of July 1, 2023.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Cybersecurity Governance

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, including attacks on critical infrastructure, and has been a target of more significant cyberattacks[2] over the last 14 years than any other country.[3] The Colonial Pipeline is an example of critical infrastructure that was attacked, disrupting what is arguably the nation's most important fuel conduit.[4]

Ransomware is a type of cybersecurity incident where malware[5] that is designed to encrypt files on a device and renders the files and the systems that rely on them unusable. In other words, critical information is no longer accessible. During a ransomware attack, malicious actors demand a ransom in exchange for regained access through decryption. If the ransom is not paid, the ransomware actors will often threaten to sell or leak the data or authentication information. Even if the ransom is paid, there is no guarantee that the bad actor will follow through with decryption.

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

Information Technology and Cybersecurity Management

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

---

[1] Cybercrime Magazine, *Cybercrime to Cost the World $8 Trillion Annually in 2023*, https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/ (last visited March 7, 2023).
[2] "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. FRA Conferences, *Study: U.S. Largest Target for Significant Cyber-Attacks*, https://www.fraconferences.com/insights-articles/compliance/study-us-largest-target-for-significant-cyber-attacks/#:~:text=The%20United%20States%20has%20been%20on%20the%20receiving,article%20is%20from%20FRA%27s%20sister%20company%2C%20Compliance%20Week (last visited Mar. 20, 2023).
[3] *Id*.
[4] S&P Global, *Pipeline operators must start reporting cyberattacks to government: TSA orders*, https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/electric-power/052721-pipeline-operators-must-start-reporting-cyberattacks-to-government-tsa-orders?utm_campaign=corporatepro&utm_medium=contentdigest&utm_source=esgmay2021 (last visited Mar. 8, 2023).
[5] "Malware" means hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. https://csrc.nist.gov/glossary/term/malware (last visited Mar 16, 2023).
[6] Cybersecurity and Infrastructure Agency, *Ransomware 101,* https://www.cisa.gov/stopransomware/ransomware-101 (last visited January 30, 2022).
[7] Tallahassee Democrat, *TMH says it has taken 'major step' toward restoration after cybersecurity incident* (Feb. 15, 2023) https://www.tallahassee.com/story/news/local/2023/02/14/tmh-update-hospital-has-taken-major-step-toward-restoration/69904510007/ (last visited Mar. 7, 2023).
[8] The term "information technology" means equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form. S. 282.0041(19), F.S.
[9] *See* s. 20.22, F.S.
[10] Ch. 2020-161, L.O.F.
[11] *See* s. 20.22(2)(b), F.S.

The head of FLDS is appointed by the Secretary of Management Services[12] and serves as the state chief information officer (CIO).[13] The CIO must have at least five years of experience in the development of IT system strategic planning and IT policy and, preferably, have leadership-level experience in the design, development, and deployment of interoperable software and data solutions.[14] FLDS must propose innovative solutions that securely modernize state government, including technology and information services, to achieve value through digital transformation and interoperability, and to fully support Florida's cloud first policy.[15]

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

- Develop IT policy for the management of the state's IT resources;
- Develop an enterprise architecture;
- Establish project management and oversight standards with which state agencies must comply when implementing IT projects;
- Perform project oversight on all state agency IT projects that have a total cost of $10 million or more and that are funded in the General Appropriations Act or any other law; and
- Identify opportunities for standardization and consolidation of IT services that support interoperability, Florida's cloud first policy, and business functions and operations that are common across state agencies.[16]

Information Technology Security Act

In 2021, the Legislature passed the IT Security Act,[17] which requires DMS and the state agency[18] heads to meet certain requirements in order to enhance the IT security of the state agencies. Specifically, the IT Security Act provides that DMS is responsible for establishing standards and processes consistent with accepted best practices for IT security,[19] including cybersecurity, and adopting rules that safeguard an agency's data, information, and IT resources to ensure availability, confidentiality, integrity, and to mitigate risks.[20] In addition, DMS must:

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

State Cybersecurity Act

In 2022, the Legislature passed the State Cybersecurity Act,[22] which requires DMS and the heads of the state agencies[23] to meet certain requirements to enhance the cybersecurity[24] of the state agencies.

[12] The Secretary of Management Services serves as the head of DMS and is appointed by the Governor, subject to confirmation by the Senate. S. 20.22(1), F.S.
[13] S. 282.0051(2)(a), F.S.
[14] *Id.*
[15] S. 282.0051(1), F.S.
[16] *Id*.
[17] S. 282.318, F.S.
[18] The term "state agency" means any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include university boards of trustees or state universities. S. 282.0041(33), F.S. For purposes of the IT Security Act, the term includes the Department of Legal Affairs, The Department of Agriculture and Consumer Services, and the Department of Financial Services. S. 282.318(2), F.S.
[19] The term "information technology security" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of data, information, and information technology resources. S. 282.0041(22), F.S.
[20] S. 292.318(3), F.S.
[21] *Id.*
[22] S. 282.318, F.S.
[23] For purposes of the State Cybersecurity Act, the term "state agency" includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services. S. 282.318(2), F.S.
[24] "Cybersecurity" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of data, information, and information technology resources. S. 282.0041(8), F.S.

DMS is tasked with completing the following, through FLDS:

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

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

- Establish a cybersecurity incident response team with FLDS and the Cybercrime Office, which must immediately report all confirmed or suspected incidents to the CISO;
- Annually submit to DMS the state agency's strategic and operational cybersecurity plans;
- Conduct and update a comprehensive risk assessment to determine the security threats;
- Develop and update written internal policies and procedures for reporting cyber incidents;
- Implement safeguards and risk assessment remediation plans to address identified risks;
- Ensure internal audits and evaluations of the agency's cybersecurity program are conducted;
- Ensure that the cybersecurity requirements for the solicitation, contracts, and service-level agreement of IT and IT resources meet or exceed applicable state and federal laws, regulations, and standards for cybersecurity, including the National Institute of Standards and Technology (NIST)[30] cybersecurity framework;
- Provide cybersecurity training to all agency employees within 30 days of employment; and
- Develop a process that is consistent with the rules and guidelines established by FLDS for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents.[31]

Florida Cybersecurity Advisory Council

[25] "Data" means a subset of structured information in a format that allows such information to be electronically retrieved and transmitted. S. 282.0041(9), F.S.
[26] "Information technology resources" means data processing hardware and software and services, communications, supplies, personnel, facility resources, maintenance, and training. S. 282.0041(22), F.S.
[27] "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security, policies, or practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur. S. 282.0041(19), F.S.
[28] S. 282.318(3), F.S.
[29] S. 282.318(4)(a), F.S.
[30] NIST, otherwise known as the National Institute of Standards and Technology, "is a non-regulatory government agency that develops technology, metrics, and standards to drive innovation and economic competitiveness at U.S.-based organizations in the science and technology industry." Nate Lord, *What is NIST Compliance*, DataInsider (Dec. 1, 2020), https://www.digitalguardian.com/blog/what-nist-compliance (last visited Mar. 17, 2023).
[31] S. 282.318(4), F.S.

The Florida Cybersecurity Advisory Council[32] (CAC) within DMS[33] assists state agencies in protecting IT resources from cyber threats and incidents.[34] The CAC must assist FLDS in implementing best cybersecurity practices, taking into consideration the final recommendations of the Florida Cybersecurity Task Force – a task force created to review and assess the state's cybersecurity infrastructure, governance, and operations.[35] The CAC meets at least quarterly to:

- Review existing state agency cybersecurity policies;
- Assess ongoing risks to state agency IT;
- Recommend a reporting and information sharing system to notify state agencies of new risks;
- Recommend data breach simulation exercises;
- Assist FLDS in developing cybersecurity best practice recommendations; and
- Examine inconsistencies between state and federal law regarding cybersecurity.[36]

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

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:

- 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.

State Data Center

In 2022, legislation moved the State Data Center (SDC) from FLDS to DMS, which now operates and maintains the SDC. 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.[38] 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) 20000, 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.[39] This allows for NWRDC to provide services from the SDC

[32] Under Florida law, an "advisory council" means an advisory body created by specific statutory enactment and appointed to function on a continuing basis. Generally, an advisory council is enacted to study the problems arising in a specified functional or program area of state government and to provide recommendations and policy alternatives. S. 20.03(7), F.S.; *See also* s. 20.052, F.S.
[33] S. 282.319(1), F.S.
[34] S. 282.319(2), F.S.
[35] S. 282.319(3), F.S.
[36] S. 282.319(9), F.S.
[37] S. 282.319(10), F.S.
[38] S. 282.201(1), F.S.
[39] S. 282.201(5), F.S.

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.[40]

Cyber Incident Response

The National Cyber Incident Response Plan (NCIRP) was developed according to the direction of Presidential Policy Directive (PPD)-41,[41] by the U.S. Department of Homeland Security. The NCIRP is part of the broader National Preparedness System and establishes the strategic framework for a whole-of-Nation approach to mitigating, responding to, and recovering from cybersecurity incidents posing risk to critical infrastructure.[42] The NCIRP was developed in coordination with federal, state, local, and private sector entities and is designed to interface with industry best practice standards for cybersecurity, including the NIST Cybersecurity Framework.

The NCIRP adopted a common schema for describing the severity of cybersecurity incidents affecting the U.S. The schema establishes a common framework to evaluate and assess cybersecurity incidents to ensure that all departments and agencies have a common view of the severity of a given incident; urgency required for responding to a given incident; seniority level necessary for coordinating response efforts; and level of investment required for response efforts.[43]

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.[44]

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 (CSOC).[45] The CSOC 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.[46] For state agency incidents at severity levels one and two, they must report these to the CSOC and the Cybercrime Office at FDLE as soon as possible.[47]

[40] NWRDC: Florida's Cloud Broker, *About Northwest Regional Data Center*, at https://www.nwrdc.fsu.edu/about (last visited Mar. 15, 2023).
[41] Annex for PPD-41: *U.S. Cyber Incident Coordination*, available at: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident (last visited Mar. 15, 2023).
[42] Cybersecurity & Infrastructure Security Agency, *Cybersecurity Incident Response*, available at https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response#:~:text=%20National%20Cyber%20Incident%20Response%20Plan%20%28NCIRP%29%20The,incidents%20and%20how%20those%20activities%20all%20fit%20together (last visited Mar. 15, 2023).
[43] *Id.*
[44] S. 282.318(3)(c)9.a, F.S.
[45] S. 282.318(3)(c)9.c, F.S.
[46] S. 282.318(3)(c)9.c.(II), F.S.
[47] S. 282.318(3)(c)(9)(d), F.S.

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

- A summary of the facts surrounding the cybersecurity or ransomware incident;
- The date on which the state agency or local government most recently backed up its data, the physical location of the backup, if the backup was affected, and if the backup was created using cloud computing;
- The types of data compromised by the cybersecurity or ransomware incident;
- The estimated fiscal impact of the cybersecurity or ransomware incident;
- In the case of a ransomware incident, the details of the ransom demanded; and
- If the reporting entity is a local government, a statement requesting or declining assistance from the CSOC, FDLE Cybercrime Office, or sheriff.[48]

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.[49] 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.[50]

Legislation passed in 2022 additionally requires state agencies and local governments to submit an after-action report to FLDS within one week of the remediation of a cybersecurity or ransomware incident.[51] The report must summarize the incident, state the resolution, and any insights from the incident.

Effect of the Bill

The bill creates the "Florida Cyber Protection Act."

The bill defines the following terms:

- "As a service" means contracting with or outsourcing to a third-party of a defined role or function as a means of delivery.
- "Cloud provider" has the same meaning as provided in NIST Special Publication 800-145.
- "Independent" means, 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 FLDS.
- "Independent verification and validation" means a third-party support service that provides a completely dependent and impartial assessment of the progress and work products of a technology project from concept to business case and throughout the project lifecycle.

The bill modifies the definition of "incident" to add anything that may "jeopardize the confidentiality, integrity, or availability of an information technology system or the information the system processes, stores, or transmits."

The bill provides that DMS, through FLDS, must ensure that independent project oversight for all state agency information technology projects that have total costs of $10 million or more is performed in compliance with applicable state and federal law. Under this oversight:

- DMS cannot be considered independent for purposes of project oversight where DMS provided assistance.
- DMS shall establish appropriate contract vehicles to facilitate procurement of project oversight as a service by a state agency and ensure that the contract vehicle includes offerings that

[48] S. 282.318(3)(c)9.b, F.S.
[49] S. 282.318(3)(c)9.e, F.S.
[50] *Id*.
[51] S. 282.318(4)(k), F.S.

incorporate the ability to abide by law. Any entity providing project oversight "as a service" must provide a report to DMS.
- A state agency can request DMS to procure project oversight as a service for a project. Such procurement by DMS would not violate the requirement that the project oversight must be independent.
- DMS, acting through FLDS, must review at least quarterly project oversight reports and, upon acceptance of the contents of the reports, provide reports to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

The bill further provides that DMS, through FLDS, must create an operations committee to meet as necessary to develop collaborative efforts between agencies on cybersecurity issues. The Secretary of Management Services is to serve as the executive director of the committee, which is composed of the following members:

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

The bill authorizes DMS, through FLDS, to respond to any state agency cybersecurity incident.

The bill changes the method by which the state CIO is appointed, requiring the Governor to appoint the position subject to confirmation by the Senate. The bill removes the requirement that the CIO consult the Secretary of Management Services when appointing a state chief data officer.

The bill requires the CIO to designate a state chief technology officer (STO) who is responsible for:

- Exploring technology solutions to meet enterprise need;
- The deployments of adopted enterprise solutions;
- Compliance with the cloud first policy;
- Recommending best practices to increase the likelihood of technology project success;
- Developing strategic partnerships with the private sector; and
- Directly supporting enterprise cybersecurity and data interoperability initiatives.

The STO may acquire cloud migration as a service to implement the enterprise of the cloud-first policy.

The bill specifies that the State Data Center (SDC) shall be overseen by and accountable to DMS in consultation with the state CIO, the state chief data officer, the state chief information security officer, and the state CTO. The bill shifts authority from DMS to FLDS to appoint the SDC director. Under the bill, a procurement or purchase of enterprise architecture by the SDC that is comparable to a project subject to requirements under s. 282.0051(4), F.S., if the total project cost is $10 million or more and may be consumed by an enterprise, must be provided to DMS and FLDS to review before publication.

The bill provides that the state CIO must assume responsibility for the contract between DMS and the Northwest Regional Data Center (NWRDC), and the NWRDC must provide FLDS with access to information regarding operations of the SDC.

Under the bill, the SDC and any successor entity assuming the responsibilities of the SDC, including NWRDC, must provide FLDS with full access to any infrastructure, system, application, or other means

that hosts, supports, or manages data in the custody of an enterprise, which must fully integrate with the Cybersecurity Operations Center (CSOC).

The bill requires the SDC and any successor entity to submit a quarterly report to DMS and FLDS that provides, relating to infrastructure servicing enterprise customers and data, the number of:

- Technology assets within 1 year of the end of life as defined by the manufacturer;
- Technology assets which are beyond end of life as defined by the manufacturer;
- Technology assets which are within 2 years of being unsupported by manufacturer;
- Technology assets which are currently unsupported by the manufacturer;
- Workloads which are hosted by a commercial cloud service provider as defined in NIST publication 500-292; and
- Service level disruptions and average duration of disruption.

The bill provides that state agencies and local governments must report ransomware or cybersecurity incidents of all security levels and adds FLDS to the list of entities that must receive such reports. Such reports must be made as soon as possible but no later than four hours after discovery of a cybersecurity incident and no later than two hours after discovery of a ransomware incident. Furthermore, the bill requires FLDS to notify the Governor, President of the Senate, and the Speaker of the House of any incident discovered by a state agency but not timely reported.

The bill requires that heads of state agencies:

- Designate a chief information security officer to integrate the agency's technical and operational cybersecurity efforts with the Cybersecurity Operations Center. This must be done annually in writing to FLDS by January 1. An agency's chief information security officer must report to the agency's chief information officer. An agency can request DMS to procure a chief information security officer as a service to fulfill these duties.
- Designate an information security manager to ensure compliance with cybersecurity governance and comply with the state's incident response plan.
- In establishing an agency cybersecurity team, incorporate the resources of the Florida State Guard as appropriate.
- Sign an annual comprehensive risk assessment facilitated by DMS. This assessment must comply with the criteria, methodology, and cope developed by the state chief information security officer. The findings must also be signed by FLDS.

The bill establishes an annual reporting deadline of January 15th for DMS to submit a report to the Governor, President of the Senate, and the Speaker of the House on alternative standards that do not conflict with federal regulations or requirements.

The bill removes the requirement that the Florida Cybersecurity Advisory Council must include a representative from a water treatment facility.

The bill creates a career service exemption for particular positions. The bill exempts personnel who are employed by or report to the CIO, state chief data officer, a chief information security officer, and an agency information security manager.

Under the bill, DMS, through FLDS, must provide cybersecurity briefings to members of any legislative committee or subcommittee responsible for policy matters relating to cybersecurity. Further, the bill allows any legislative committee or subcommittee responsible for policy matters relating to cybersecurity to hold meetings closed under the rules of the legislative body when such committee or subcommittee is briefed on records made confidential and exempt. The committee and subcommittee must maintain the confidential and exempt status of the records.

Limitation on Liability

Present Situation

Access to Courts

The Florida Constitution broadly protects the right to access the courts, which "shall be open to every person for redress of any injury..."[52] However, this constitutional right is not unlimited.

In *Kluger v. White*,[53] the Court stated that it would not completely prohibit the Legislature from altering a cause of action, but neither would it allow the Legislature "to destroy a traditional and long-standing cause of action upon mere legislative whim..." The takeaway from *Kluger* and other relevant case law is that the Legislature may:

- Reduce the right to bring a cause of action as long as the right is not entirely abolished.[54]
- Abolish a cause of action that is not "traditional and long-standing"—that is, a cause of action that did not exist at common law, and that did not exist in statute before the adoption of the Florida Constitution's Declaration of Rights.[55]
- Abolish a cause of action if the Legislature either:
    - Provides a reasonable commensurate benefit in exchange;[56] or
    - Shows an "overpowering public necessity for the abolishment of such right, and no alternative method of meeting such public necessity can be shown."[57]

Tort Liability and Negligence

A "tort" is a wrong for which the law provides a remedy. The purpose of tort law is to fairly compensate a person harmed by another person's wrongful acts, whether intentional, reckless, or negligent, through a civil action or other comparable process. A properly-functioning tort system:

- Provides a fair and equitable forum to resolve disputes;
- Appropriately compensates legitimately harmed persons;
- Shifts the loss to responsible parties;
- Provides an incentive to prevent future harm; and
- Deters undesirable behavior.[58]

"Negligence" is a legal term for a type of tort action that is unintentionally committed. In a negligence action, the plaintiff is the party that brings the lawsuit, and the defendant is the party that defends against it. To prevail in a negligence lawsuit, a plaintiff must demonstrate that the:

- Defendant had a legal duty of care requiring the defendant to conform to a certain standard of conduct for the protection of others, including the plaintiff, against unreasonable risks;
- Defendant breached his or her duty of care by failing to conform to the required standard;
- Defendant's breach caused the plaintiff's injury; and
- Plaintiff suffered actual damage or loss resulting from his or her injury.[59]

Courts distinguish varying degrees of civil negligence by using terms such as:

---

[52] Art. I, s. 21, Fla. Const.
[53] *Kluger*, 281 So. 2d 1.
[54] *See Achord v. Osceola Farms Co.*, 52 So. 3d 699 (Fla. 2010).
[55] *See Anderson v. Gannett Comp.*, 994 So. 2d 1048 (Fla. 2008) (false light was not actionable under the common law); *McPhail v. Jenkins*, 382 So. 2d 1329 (Fla. 1980) (wrongful death was not actionable under the common law); *see also Kluger*, 281 So. 2d at 4 ("We hold, therefore, that where a right of access to the courts for redress for a particular injury has been provided by statutory law predating the adoption of the Declaration of Rights of the Constitution of the State of Florida, or where such right has become a part of the common law of the State . . . the Legislature is without power to abolish such a right without providing a reasonable alternative . . . unless the Legislature can show an overpowering public necessity. . .").
[56] *Kluger*, 281 So. 2d at 4; *see Univ. of Miami v. Echarte*, 618 So. 2d 189 (Fla. 1993) (upholding a statutory cap on medical malpractice damages because the Legislature provided arbitration, which is a "commensurate benefit" for a claimant); *accord Lasky v. State Farm Ins. Co.*, 296 So. 2d 9 (Fla. 1974); *but see Smith v. Dept. of Ins.*, 507 So. 2d 1080 (Fla. 1992) (striking down a noneconomic cap on damages, which, while not wholly abolishing a cause of action, did not provide a commensurate benefit).
[57] *Kluger*, 281 So. 2d at 4-5 (noting that in 1945, the Legislature abolished the right to sue for several causes of action, but successfully demonstrated "the public necessity required for the total abolition of a right to sue") (citing *Rotwein v. Gersten*, 36 So. 2d 419 (Fla. 1948); *see Echarte*, 618 So. 2d at 195 ("Even if the medical malpractice arbitration statutes at issue did not provide a commensurate benefit, we would find that the statutes satisfy the second prong of *Kluger* which requires a legislative finding that an 'overpowering public necessity' exists, and further that 'no alternative method of meeting such public necessity can be shown'").
[58] Am. Jur. 2d Torts s. 2.
[59] 6 *Florida Practice Series* s. 1.1; *see Barnett v. Dept. of Financial Services*, 303 So. 3d 508 (Fla. 2020).

Slight Negligence	The failure to exercise great care. This often applies to injuries caused by common carries charged with the duty to exercise the highest degree of care toward their passengers.[60]
Ordinary Negligence	The failure to exercise that degree of care which an ordinary prudent person would exercise; or, in other words, a course of conduct which a reasonable and prudent person would know might possibly result in injury to others.[61]
Gross Negligence	A course of conduct which a reasonable and prudent person knows would probably and most likely result in injury to another.[62] To prove gross negligence, a plaintiff must usually show that the defendant had knowledge or awareness of imminent danger to another and acted or failed to act with a conscious disregard for the consequences.[63] Once proven, gross negligence may support a punitive[64] damages award.[65]

In Florida, before a court awards damages in a negligence action, the jury generally assigns a fault percentage to each party under the comparative negligence rule. Florida applies[66] a "pure" comparative negligence rule, which allows a plaintiff to recover damages proportional to his or her fault percentage.[67] For example, if a plaintiff is 40 percent at fault for an accident causing the plaintiff's injury and the defendant is 60 percent at fault, the plaintiff would recover 60 percent of his or her damages.

The Florida Rules of Civil Procedure generally require a plaintiff in a civil action to file a complaint, and require a defendant to file an answer to the complaint.[68] Florida is a "fact-pleading jurisdiction." This means that a pleading setting forth a claim for relief, including a complaint, must generally state a cause of action and contain a:

- Short and plain statement of the grounds on which the court's jurisdiction depends, unless the court already has jurisdiction and the claim needs no new grounds to support it;
- Short and plain statement of the ultimate facts[69] showing the pleader is entitled to relief; and
- Demand for the relief to which the pleader believes he or she is entitled to.[70]

However, certain allegations[71] must be plead with "particularity," which is a heightened level of pleading requiring a statement of facts sufficient to satisfy the elements of each claim.

Burden of Proof and Presumptions

The burden of proof is an obligation to prove a material fact in issue.[72] Generally, the party who asserts the material fact in issue has the burden of proof.[73] In a civil proceeding, for example, the burden of proof is on the plaintiff to prove the allegations contained in his or her complaint. Further, a defendant in

[60] *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.
[61] *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.
[62] *See Clements*, 88 So. 2d 505; 6 *Florida Practice Series* s. 1.2.
[63] *See Carraway v. Revell*, 116 So. 2d 16 (Fla. 1959).
[64] Punitive damages are awarded in addition to actual damages to punish a defendant for behavior considered especially harmful. Florida generally caps punitive damage awards at $500,000 or triple the value of compensatory damages, whichever is greater, and caps cases of intentional misconduct with a financial motivation at two million dollars or four times the amount of compensatory damages, whichever is greater. S. 768.73(1), F.S.
[65] *See Glaab v. Caudill*, 236 So. 2d 180 (Fla. 2d DCA 1970); 6 *Florida Practice Series* s. 1.2; s. 768.72(2), F.S.
[66] The comparative negligence standard does not apply to any action brought to recover economic damages from pollution, based on an intentional tort, or to which the joint and several liability doctrines is specifically applied in chs. 403, 498, 517, 542 , and 895, F.S. S. 768.81(4), F.S.
[67] S. 768.81(2), F.S.; *see Williams v. Davis*, 974 So. 2d 1052 (Fla. 2007).
[68] Fla. R. Civ. P. 1.100.
[69] Ultimate facts are facts that must be accepted for a claim to prevail, usually inferred from a number of supporting evidentiary facts, which themselves are facts making other facts more probable. *See* Legal Information Institute, *Ultimate Fact*, https://www.law.cornell.edu/wex/ultimate_fact (last visited Mar. 16, 2023); *see also* Legal Information Institute, *Evidentiary Facts*, https://www.law.cornell.edu/wex/evidentiary_fact (last visited Mar. 16, 2023).
[70] *See Goldschmidt v. Holman*, 571 So. 2d 422 (Fla. 1990); Fla. R. Civ. P. 1.110.
[71] These allegations include fraud, mistake, condition of the mind, and denial of performance or occurrence. Fla. R. Civ. P. 1.120(b),(c).
[72] 5 *Florida Practice Series* s. 16:1.
[73] *Id.*; *see Berg v. Bridle Path Homeowners Ass'n, Inc.*, 809 So. 2d 32 (Fla. 4th DCA 2002).

either a criminal or a civil proceeding has the burden to prove any affirmative defenses[74] he or she may raise in response to the charges or allegations. However, there are certain statutory and common law presumptions[75] that may shift the burden of proof from the party asserting the material fact in issue to the party defending against such fact.[76] 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.[77] 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.[78]

Cybersecurity Standards

Per Florida law, 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.[79] The standards must be consistent with generally accepted best practices for cybersecurity, including the NIST cybersecurity framework.[80] Once the standards are adopted, each local government is to notify FLDS as soon as possible.[81]

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.[82] The framework is designed to complement, and not replace, an organization's own unique 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.[83] Other cybersecurity standards include:

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.[84]
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.[85]

[74] An affirmative defense is a defense which, if proven, negates criminal or civil liability even if it is proven that the defendant committed the acts alleged. Examples include self-defense, entrapment, insanity, necessity, and *respondeat superior*. Legal Information Institute, *Affirmative Defense*, https://www.law.cornell.edu/wex/affirmative_defense (last visited Mar. 16, 2021).
[75] 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.
[76] 5 *Florida Practice Series* s. 16:1.
[77] *Id.*
[78] Legal Information Institute, *Presumption*, https://www.law.cornell.edu/wex/presumption (last visited Mar. 16, 2023).
[79] S.282.3185(4)(a), F.S.
[80] *Id*.
[81] S.282.3185(4)(d), F.S.
[82] 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 7, 2023).
[83] *Id.*
[84] 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. 15, 2023).
[85] 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. 16, 2023).

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).[86]
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.[87]
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.[88]

[86] 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. 16, 2023).
[87] CIS Security, *CIS Critical Security Controls*, https://www.cisecurity.org/controls (last visited Mar. 16, 2023).
[88] 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. 16, 2023).

Effect of the Bill

The bill provides that specified entities that substantially comply with certain standards are not liable in connection with a cybersecurity incident.

Under the bill, a county or municipality that substantially complies with s. 282.3185, F.S., is not liable in connection with a cybersecurity incident. The bill also provides that a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity acquires, maintains, stores, or uses personal information is not liable if the entity substantially complies with s. 501.171, F.S., and has adopted a cybersecurity program that substantially aligns with the current version of any of the following:

- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity;
- NIST special publication 800-171;
- NIST special publications 800-53 and 800-53A;
- The Federal Risk and Authorization Management Program security assessment framework;
- CIS Critical Security Controls; or
- The International Organization for Standardization/International Electrotechnical Commission 27000 – series family of standards.

Under the bill, if the entity is regulated by the state or federal government, or both, or if otherwise subject to the requirements of any of the following laws and regulations, it must substantially comply its cybersecurity program to the current version of:

- The security requirements of the Health Insurance Portability and Accountability Act of 1996;
- Title V of the Gramm-Leach-Bliley Act of 1999 as amended;
- The Federal Information Security Modernization Act of 2014; or
- The Health Information Technology for Economic and Clinical Health Act.

The bill provides that the specified non-governmental entities must base their compliance with one of the standards off of these factors:

- The size and complexity of the covered entity;
- The nature and scope of the activities of the covered entity; and
- The sensitivity of the information to be protected.

Under the bill, any commercial entity that substantially complies with a combination of industry-recognized cybersecurity frameworks or standards, including the payment card industry data security standard, gains a presumption against liability and must adopt the revised frameworks or standards within 1 year after the latest publication date stated in the revisions.

The bill does not establish a private cause of action. It provides that a failure of a county, municipality, or commercial entity to substantially implement a cybersecurity program that would allow it to gain a presumption against liability under the bill is not evidence of negligence and does not constitute negligence per se. In an action in connection to a cybersecurity incident, if the defendant is an entity covered by the bill, the defendant holds the burden of proof to establish substantial compliance.

The bill provides that the act shall take effect July 1, 2023

B. SECTION DIRECTORY:

Section 1: Provides a short title for the act.

Section 2: Amends s. 110.225, F.S., relating to career service exemptions.

Section 3: Amends s. 282.0041, F.S., relating to definitions.

Section 4: Amends s. 282.0051, F.S. relating to DMS; FLDS; powers, duties, and functions.

Section 5: Amends s. 282.201, F.S., relating to the State Data Center.

Section 6: Amends s. 282.318, F.S., relating to cybersecurity.

Section 7: Amends s. 282.3185, F.S., relating to local government cybersecurity.

Section 8: Amends and adds to s. 282.319, F.S., relating to Florida Cybersecurity Advisory Council.

Section 9: Creates s. 768.401, F.S., creating a presumption against liability.

Section 10: Provides an effective date of July 1, 2023.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   The bill may require additional expenditures by the state.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

   Not applicable. This bill does not appear to require counties or municipalities to spend funds or take action requiring the expenditures of funds; reduce the authority that counties or municipalities have to raise revenues in the aggregate; or reduce the percentage of state tax shared with counties or municipalities.

2. Other:

   None.

B. RULE-MAKING AUTHORITY:

The bill does not authorize or require rulemaking.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES

On March 21, 2023, the Energy, Communications & Cybersecurity Subcommittee adopted one amendment to the bill and reported the bill favorably as a committee substitute. The amendment:

- Removed language from the bill that shifted authority related to cybersecurity governance from the Department of Management Services (DMS) to the Florida Digital Service (FLDS).
- Added and amended definitions.
- Provided DMS with additional responsibilities related to technology project oversight and cybersecurity incidents.
- Modified the membership of the operations committee required by the bill.
- Required the state CIO to designate a state chief technology officer and outlined the responsibilities of that position.
- Specified oversight of the state data center (SDC) and provided FLDS with authority to appoint the SDC director.
- Required the SDC to fully integrate with the Cybersecurity Operations Center.
- Specified information that the SDC must report to DMS and FLDS.
- Provided that the state CIO must assume responsibility for the contract between DMS and the Northwest Regional Data Center (NWRDC) and that NWRDC must provide FLDS with access to information regarding operations of the SDC.
- Required state agencies and local governments to report all ransomware incidents within 4 hours and all cybersecurity incidents within 2 hours and added FLDS to the list of entities that must receive such reports.
- Provided new requirements for heads of state agencies related to cybersecurity.
- Removed the State Technology Advancement Council created by the bill.
- Created a career service exemption for particular positions.
- Clarified application of a presumption against liability.

This analysis is drafted to the committee substitute as adopted by the Energy, Communications & Cybersecurity Subcommittee.