The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Appropriations

BILL:	CS/CS/SB 1670
INTRODUCER:	Appropriations Committee; Military and Veterans Affairs, Space, and Domestic Security Committee; and Senator Hutson
SUBJECT:	Cybersecurity
DATE:	March 2, 2022
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Lloyd	Caldwell	MS	**Fav/CS**
2.	Hunter	Sadberry	AP	**Fav/CS**

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/CS/SB 1670 modifies cybersecurity training and reporting standards for state agencies and local governments.

The State Cybersecurity Act requires the Florida Digital Service (FLDS) and the heads of state agencies to meet certain requirements to enhance the cybersecurity of state agencies. Currently, state agencies must provide cybersecurity training to their employees, report cybersecurity incidents, and adopt cybersecurity standards. However, there are no such requirements for counties and municipalities (local governments).

Current law regarding state or local government cybersecurity does not specifically address ransomware, which is a form of malware designed to encrypt files on a device, rendering any files unusable. Malicious actors then demand ransom in exchange for decryption.

The bill prohibits state agencies and local governments from paying or otherwise complying with a ransomware incident.

The bill defines the severity level of a cybersecurity incident in accordance with the National Cyber Incident Response Plan. State agencies and local governments must report all ransomware incidents and high severity level cybersecurity incidents to the Cybersecurity Operations Center (CSOC) and the Cybercrime Office within the Florida Department of Law Enforcement as soon as possible but no later than a time certain. Local governments must also report to the sheriff.

The bill requires state agencies to report low level cybersecurity incidents and provides that local governments may report such incidents. The bill also requires state agencies and local governments to submit after-action reports to the FLDS following a cybersecurity or ransomware incident.

The bill requires the CSOC to notify the Legislature of high severity level cybersecurity incidents. The notice must contain a high-level overview of the incident and its likely effects. In addition, the CSOC must provide the Legislature and the Cybersecurity Advisory Council (CAC) with a consolidated incident report on a quarterly basis.

The bill requires state agency and local government employees to undergo certain cybersecurity training within 30 days of employment and annually thereafter.

The bill requires local governments to adopt cybersecurity standards that safeguard the local government's data, information technology (IT), and IT resources.

The bill expands the purpose of the CAC to include advising local governments on cybersecurity and requires the CAC to examine reported cybersecurity and ransomware incidents to develop best practice recommendations. The CAC must submit an annual comprehensive report regarding ransomware to the Governor and Legislature.

The bill establishes penalties and fines for certain ransomware offenses against a government entity.

The bill will likely have a negative fiscal impact on state and local government expenditures; however, the bill may also have a positive fiscal impact on the state due to the punitive fine established in the bill. See Fiscal Analysis & Economic Impact Statement.

The bill's effective date is July 1, 2022.

II. Present Situation:

General Background

Ransomware is a form of malware[1] that is used by malicious actors to encrypt files on devices, networks, or computer systems, rendering the files on those systems unusable. The malicious actors then demand ransom in exchange for decryption or the return of an individual's or an organization's files. Ransomware actors will also often threaten to sell or leak the data or information if the demanded ransom is not paid.

The number of ransomware incidents continues to rise, with 2,474 incidents reported with adjusted losses of over $29.1 million,[2] a figure that is likely under-inclusive, as technology

[1] "Malware" means hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. *See* *https://csrc.nist.gov/glossary/term/malware* (last visited Feb. 4, 2022).
[2] Federal Bureau of Investigation, Internet Crime Complaint Center, 2020 Internet Crime Report, Business Email Compromise (BEC), p.14, *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Feb. 2, 2022).

experts believe that many ransomware attacks go unreported out of embarrassment by victims who decline to report. In its reporting, the Federal Bureau of Investigation (FBI) formally describes ransomware as:

> A type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cybercriminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.[3]

The Internet Crime Complaint Center (IC3), housed within the FBI received a record number of complaints from the American public in 2020: 791,790, with the reported losses attached to those complaints exceeding $4.1 billion.[4] This represents a 69 percent increase in total complaints from 2019.

Recent ransomware attacks that impacted the American economy include:

- The Colonial Pipeline shutdown in May 2021, which disrupted the flow of refined gasoline and jet fuel through 5,500 miles of pipeline from Texas to New York.[5]
  - Colonial supplied 45 percent of the East Coast's fuel supply.
  - As a private company, Colonial had no duty to report; however, the FBI and federal investigative agencies at the time did confirm involvement in the investigation.[6]
  - A ransom of 75 Bitcoin was paid a day after Colonial's network system was breached, and a total ransom, which was the equivalent of nearly $5 million in cryptocurrency was eventually paid for the software decryption key to unlock its networks.[7]
- JBS, the world's largest meat processing plant, was hit by a ransomware attack in June 2021:[8]
  - The plant is responsible for supplying one quarter of America's beef.[9]
  - The likely Russian-based hackers threatened disruption or deletion of network files unless a ransom was paid.
  - Ultimately, JBS paid a ransom in Bitcoin of $11 million to resolve the cyberattack.[10]

Specifically, in Florida, recent cybersecurity and ransomware incidents include:

- A February 2021 intrusion into the City of Oldsmar's water system. The remote hacker briefly increased the amount of sodium hydroxide (lye) from 100 parts per million to 11,100

---

[3] *Id*.
[4] *Id*, p.3.
[5] David E. Sanger, et al, *Cyberattack forces a shutdown of a top U.S. Pipeline*, THE NEW YORK TIMES (May 13, 2021) *available at* https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html (last visited Feb. 2, 2022).
[6] *Id*.
[7, 8, 9] Associated Press, *Colonial Pipeline confirms it paid $4.4m to hacker gang after attack* (May 19, 2021), THE GUARDIAN, *available at* https://www.theguardian.com/technology/2021/may/19/colonial-pipeline-cyber-attack-ransom (last visited Jan. 23, 2022).
[8] *JBS: Cyber-Attack hits world's largest meat supplier*, BBC.COM, *available at* https://www.bbc.com/news/world-us-canada-57318965 (last visited Jan. 22, 2022).
[9] *Id*.
[10] *Meat Giant JBS pays $11m in ransom to resolve cyberattack*, BBC.COM, *available at* https://www.bbc.com/news/business-57423008 (last visited Jan. 23, 2022).

parts per million, more than 100 times the normal level. The increased amount was caught before the public was harmed.
- The St. Lucie County's Sheriff's Department was hit by a cyberattack in December 2020 when public records were taken and held for $1 million ransom and sheriff employees briefly resorted to filing reports using pen and paper instead.
- In Wakulla County in 2019, the school district's insurer paid a Bitcoin ransom to hackers to bring its computers back online during the first few weeks of the 2019-2020 school year.

Colonial Pipeline and JBS are just two examples from the thousands of other reports investigated by the IC3 in 2021. The United States is the number one target for cyberattacks with expected increases in both cyberattacks and particularly, ransomware attacks, according to statistics from the University of West Florida's Center for Cybersecurity.[11]

National Institute for Standards and Technology Cybersecurity Framework

The National Institute for Standards and Technology (NIST) is a non-regulatory federal agency housed within the United States Department of Commerce. The 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.[12] 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. Overall, the framework provides an outline of best practices that helps organizations decide where to focus resources for cybersecurity protection.[13]

National Cyber Incident Response Plan

The National Cyber Incident Response Plan (NCIRP) was developed according to the direction of Presidential Policy Directive (PPD)-41,[14] 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.[15] The NCIRP is not a tactical or operational plan; rather, it serves as the primary strategic framework for stakeholders to understand how federal departments and agencies and other national-level partners provide resources to support response operations. The NCIRP was developed in coordination with

---

[11] Eman El Sheikh, Ph.D., Center for Cybersecurity, University of West Florida, *Cybersecurity Education and Workforce Development Highlights (January 17, 2020 Presentation to Florida Cybersecurity Task Force Meeting, January 17, 2020), available at* CSTF_01.17.20_Meeting_Materials.pdf (myflorida.com) (last visited Jan. 23, 2022).
[12] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited Jan. 30, 2022).
[13] *Id.*
[14] 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 Feb. 18, 2022).
[15] U.S. Department of Homeland Security, *National Cyber Incident Response Plan* (December 2016) *available at file:///C:/Users/Villa.Chris/Downloads/798128% 20(7).pdf* (last visited Feb. 20, 2022).

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.[16]

Figure 1: Cybersecurity Incident Severity Schema

Disaster Level	Cyber Incident Severity	Description
Level 1	Level 5 *Emergency*	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.
Level 2	Level 4 *Severe*	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
	Level 3 *High*	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 3	Level 2 *Medium*	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
	Level 1 *Low*	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

[16] *Id.*

Florida Information Protection Act of 2014

The *Florida Information Protection Act of 2014*[17] requires notice be given to affected customers and the Department of Legal Affairs (DLA) when a breach of personal information occurs. The notice must be provided within 30 days of the discovery of the breach or the belief that a breach has occurred, unless law enforcement has requested a delay for investigative purposes or for other good cause. State law requires Florida's Attorney General to file with the Legislature, every February 1st, a report identifying any governmental entities that have reported any breaches of security of themselves or by any of its third-party agents in the preceding calendar year. Additionally, the Attorney General must report on any breaches by any governmental entities affecting more than 500 individuals in this state as expeditiously as possible, but not later than 30 days after the determination of the breach or reason to believe the breach has occurred. An extension of up to 15 days may be granted if good cause is provided in writing to the DLA.

Enforcement authority is provided to the DLA under the Florida Deceptive and Unfair Trade Practices Act to prosecute violations. Violators may be subject to civil penalties if a breach notification is not provided on a timely basis, but there are not civil penalties for the timely report of a security breach. There are exceptions for those entities that are also required to report breaches to federal regulators.

Data Breach Reporting Within Florida Law

Florida is within the FBI's top ten states for total number of victims reporting a data breach for 2020, falling behind only California with 53,793 victims[18] and is fourth in the total amount of victim loss reported at $295 million for 2020.[19]

The Attorney General's office website posts notices and news releases relating to several multi-state settlements because of data breaches which are listed through litigation settlements and press releases on the site. [20]

Information Technology Management

The Department of Management Services (DMS)[21] oversees information technology (IT)[22] governance and security for the executive branch of state government. The Florida Digital Service (FLDS) within the DMS was established by the Legislature in 2020 to replace the

[17] Ch. 2014-189, Laws of Fla. (creating s. 501.171, F.S., effective July 1, 2014; Florida Information Protection Act).
[18] *Supra,* note 2.
[19] *Id.* at 24.
[20] Office of Attorney General Ashley Moody, *In the News – News Search (search conducted January 24, 2022), available at* http://www.myfloridalegal.com/newsrel.nsf/newsreleases (last visited Jan. 24, 2022).
[21] *See* s. 20.22, F.S.
[22] The term "information technology" means equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display , store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form. Section 282.0041(20), F.S. 12 Ch. 2020-161, Laws of Fla.

Division of State Technology.[23] The head of FLDS is appointed by the Secretary of Management Services[24] and serves as the state chief information officer (CIO).[25]

The FLDS was created to 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.[26] Accordingly, the DMS through the FLDS has the following powers, duties, and functions:

- Develop IT policy for the management of the state's IT resources.
- Develop an enterprise architecture.
- Establish project management and oversight standards with which state agencies[27] must comply when implementing IT projects.
- Perform project oversight on 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.[28]
- 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.[29]

State Cybersecurity Act

The State Cybersecurity Act[30] requires the DMS and the heads of state agencies[31] to meet certain requirements to enhance the cybersecurity[32] of state agencies. Specifically, the DMS, acting through the FLDS must:

- Establish standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures consistent with generally accepted best practices for cybersecurity, including the NIST cybersecurity framework.

[23] Ch. 2020-161, Laws of Fla.
[24] The Secretary of Management Services serves as the head of the Department of Management Services (DMS) and is appointed by the Governor, subject to confirmation by the Senate. Section 20.22(1), F.S.
[25] Section 282.0051(2)(a), F.S.
[26] Section 282.0051(1), F.S.
[27] "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, state universities, the Department of Legal Affairs, the Department of Agriculture and Consumer Services, or the Department of Financial Services. Section 282.0041(33), F.S.
[28] For the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services, Florida Digital Service (FLDS) provides project oversight on information technology (IT) projects that have a total cost of $20 million or more. Section 282.0051(1)(n), F.S.
[29] Section 282.0051(1), F.S.
[30] Section 282.318, F.S.
[31] 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.
[32] "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.

- Adopt rules to mitigate risk, support a security governance framework, and safeguard state agency digital assets, data,[33] information, and IT resources[34] to ensure availability, confidentiality, and integrity.
- Designate a chief information security officer (CISO) responsible for the development, operation, and oversight of cybersecurity for state technology systems. The CISO must be notified of all confirmed or suspected incidents or threats of state agency IT resources and must report such information to the CIO and the Governor.
- Develop and annually update a statewide cybersecurity strategic plan that includes security goals and objectives for cybersecurity, including the identification and mitigation of risk, proactive protections against threats, tactical risk detection, threat reporting, and response and recovery protocols for cyber incidents.[35]
- Develop and publish for use by state agencies a cybersecurity governance framework.
- Assist state agencies in complying with the State Cybersecurity Act.
- In collaboration with the Cybercrime Office within the Florida Department of Law Enforcement (FDLE), annually provide training for state agency information security managers and computer security incident response team members that contains training on cybersecurity, including cybersecurity threats, trends, and best practices.
- Annually review the strategic and operational cybersecurity plans of state agencies.
- Track, in coordination with agency inspectors general, 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. The training may be provided in collaboration with the Cybercrime Office, a private sector entity, or an institution of the state university system.
- Operate and maintain a Cybersecurity Operations Center led by the CISO to serve as a clearinghouse for threat information and to coordinate with the FDLE to support state agency response to cybersecurity incidents.
- Lead an Emergency Support Function under the state comprehensive emergency management plan.[36]

The State Cybersecurity Act requires the head of each state agency to designate an information security manager to administer the cybersecurity program of the state agency.[37] In addition, the head of each state agency must:

- Establish an agency cybersecurity incident response team in consultation with FLDS and the Cybercrime Office. The agency cybersecurity incident response team must convene upon notification of a cybersecurity incident and must immediately report all confirmed or suspected incidents to the CISO.

[33] "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.
[34] "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.
[35] "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.
[36] Section 282.318(3), F.S.
[37] Section 282.318(4)(a), F.S.

- Annually submit to the DMS the state agency's strategic and operational cybersecurity plans.
- Conduct and update every three years a comprehensive risk assessment to determine the security threats to the data, information, and IT resources of the state agency.
- Develop and periodically update written internal policies and procedures, including procedures for reporting cybersecurity incidents and breaches to the FLDS and the Cybercrime Office.
- Implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended by the DMS to address identified risks to the data, information, and IT resources of the agency.
- Ensure that periodic internal audits and evaluations of the agency's cybersecurity program for the data, information, and IT resources of the agency are conducted.
- Ensure that the cybersecurity requirements included as written specifications within a solicitation, contract, and service-level agreement of IT and IT resources and services meet or exceed applicable state and federal laws, regulations, and standards for cybersecurity, including the NIST cybersecurity framework.
- Provide cybersecurity awareness training to all state agency employees within 30 days of commencing employment concerning cybersecurity risks and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the state agency to reduce those risks. The training may be provided in collaboration with the Cybercrime Office, a private sector entity, or an institution of the state university system.
- Develop a process that is consistent with the rules and guidelines established by the FLDS for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents.[38]

Florida Cybersecurity Advisory Council

The Florida Cybersecurity Advisory Council (CAC) within the DMS[39] assists state agencies in protecting IT resources from cyber threats and incidents.[40] 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.[41] The CAC meets at least quarterly to:

- Review existing state agency cybersecurity policies.
- Assess ongoing risks to state agency IT.
- Recommend a reporting and information sharing system to notify state agencies of new risks.
- Recommend data breach simulation exercises.
- Assist the FLDS in developing cybersecurity best practice recommendations for state agencies, including continuous risk monitoring, password management, and protecting data in legacy and new systems.
- Examine inconsistencies between state and federal law regarding cybersecurity.[42]

The CAC must work with the NIST and other federal agencies, private sector businesses, and private security experts to identify which local infrastructure sectors, not covered by federal law,

[38] Section 282.318(4), F.S.
[39] Section 282.319(1), F.S.
[40] Section 282.319(2), F.S.
[41] Section 282.319(3), F.S.
[42] Section 282.319(9), F.S.

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.[43]

Beginning June 30, 2022, and each June 30 thereafter, the CAC must submit to the Legislature any recommendations considered necessary by the CAC to address cybersecurity.[44]

Offenses against Users of Computers

Florida law criminalizes the following acts involving a computer,[45] computer system,[46] computer network,[47] or electronic device[48] when done knowingly, willfully, and without authorization:

- Accessing[49] or causing to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized or the manner or use exceeds authorization.
- Disrupting or denying the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device under certain circumstances.
- Destroying, taking, injuring, or damaging computers, computer systems, computer networks, or electronic devices.
- Introducing a computer contaminant into a computer, computer system, computer network, or electronic device.
- Engaging in audio or video surveillance of an individual by accessing one of the inherent features or components of a computer, computer system, computer network, or electronic device, including accessing the data or information stored by a third party.[50]

[43] Section 282.319(10), F.S.
[44] Section 282.319(11), F.S.
[45] "Computer" means an internally programmed, automatic device that performs data processing. Section 815.03(2), F.S.
[46] "Computer system" means a device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control. The term does not include calculators that are not programmable and that are not capable of being used in conjunction with external files. Section 815.03(7), F.S.
[47] "Computer network" means a system that provides a medium for communication between one or more computer systems or electronic devices, including communication with an input or output device such as a display terminal, printer, or other electronic equipment that is connected to the computer systems or electronic devices by physical or wireless telecommunication facilities. Section 815.03(4), F.S.
[48] "Electronic device" means a device or a portion of a device that is designed for and capable of communicating across a computer network with other computers or devices for the purpose of transmitting, receiving, or storing data, including, but not limited to, a cellular telephone, tablet, or other portable device designed for and capable of communicating with or across a computer network and that is actually used for such purpose. Section 815.03(9), F.S.
[49] "Accessing" means approaching, instructing, communicating with, storing data in, retrieving data from, or otherwise making use of any resources of a computer, computer system, computer network, or electronic device. Section 815.03(1), F.S.
[50] Section 815.06(2), F.S.

In general, such conduct against a computer user is a third degree felony,[51] punishable by up to five years in prison and a $5,000 fine.[52] However, the crime may be enhanced to a second[53] or first[54] degree felony with aggravating factors, such as excessive damage or endangering a human life.[55]

Unfunded Local Government Mandates

An unfunded mandate on local government is defined in Florida's Constitution as a general law which requires counties or municipalities to spend its funds, limits their ability to raise revenue, or limits their ability to receive sales tax revenue. Adopted by Florida voters in 1990, Article VII, Section 18(a) of the Florida Constitution states that no county or municipality shall be bound by any general law requiring such county or municipality to spend its funds or to take an action requiring the expenditure of funds except under certain conditions. The review process is only applied to general laws applicable to cities and counties and not to special districts or school districts.

Article VII, s. 18 of the Florida Constitution requires also that such laws fulfill an important state interest and meet one of the following conditions for constitutionality:

- The Legislature has provided or will provide the estimated amount of funds necessary to fund the mandated activity or program;
- The Legislature has provided or will provide the county or municipality the authorization to enact a funding source not available to them before February 1, 1989, that can be used to generate the amount of funds sufficient to meet the mandate by a simple majority vote for the governing body;
- The law passes by a two-thirds membership vote of each house of the Legislature;
- The expenditure is required to comply with a law that applies to all persons similarly situated, including the state and local governments; or
- The law is required to comply with a federal requirement or is required to comply with a federal entitlement.

If none of the constitutional exceptions or exemptions apply, and if the bill becomes law, cities and counties are not bound by the law[56] unless the Legislature has determined that the bill fulfills an important state interest and approves the bill by a two-thirds vote of the membership of each house. A Legislature can meet the condition "meets an important state interest" through a legislative declaration and a declaratory statement that the legislation does meet an important state interest.

[51] Section 815.06(3)(a), F.S.
[52] Section 775.082 and 775.083, F.S.
[53] A second degree felony is punishable by up to 15 years in prison and a $10,000 fine. Sections 775.082 and 775.083, F.S.
[54] A first degree felony is punishable by up to 30 years in prison and a $10,000 fine. Sections 775.082 and 775.083, F.S.
[55] Section 815.06(3)(b) and (3)(c), F.S.
[56] Although the constitution says, "[n]o county or municipality shall be bound by any general law" that is a mandate, the circuit court's ruling was much broader in that it ordered SB 360 expunged completely from the official records of the state.

A mandate can still be prohibited if the effect of its enactment results in a reduction in the county or municipality's authority to raise total aggregate revenues or is a reduction in the total percentage share of revenue as it existed on February 1, 1989.

Mandates can be exempted in certain circumstances, such as, if the law is being enacted during a declared fiscal emergency, when offsetting revenues are provided for, or when the fiscal impact is considered insignificant. The Legislature interprets insignificant fiscal impact to mean an amount not greater than the average statewide population for the applicable fiscal year times 10 cents (currently $2.3 million); the average fiscal impact, including any offsetting effects over the long term, is also considered.[57]

III. Effect of Proposed Changes:

Ransomware Incident

The bill defines "ransomware incident" to mean a malicious cybersecurity incident in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a state agency's or local government's[58] data and thereafter the person or entity demands a ransom to restore access to the data, prevent publication of the data, or otherwise remediate the impact of the software. The bill prohibits a state agency or local government experiencing a ransomware incident from paying or otherwise complying with the demanded ransom.

Cybersecurity and Ransomware Incident Notification

The bill defines the severity level of a cybersecurity incident in accordance with the National Cyber Incident Response Plan (NCIRP) 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.

[57] Guidelines issued in 1991 by then-Senate President Gwen Margolis and Speaker of the House Wetherell (1991); Comm. On Comprehensive Planning, Local and Military Affairs, The Florida Senate, *Review of Legislative Staff Guidelines for Screening Bills for Mandates on Florida Counties and Municipalities* (Interim Report 2000-24)(Sept. 1999), *available at* http://www.leg.state.fl.us/data/Publications/2000/Senate/reports/interim_reports/pdf/00-24ca.pdf (last visited Jan. 26, 2022).
[58] The bill defines "local government" to mean a county or a municipality.

The bill requires state agencies and local governments to report all ransomware incidents as soon as possible, but no later than 12 hours after discovery of the incident. It also requires state agencies and local governments to report cybersecurity incidents determined to be of severity level three, four, or five as soon as possible, but no later than 48 hours after discovery of the incident. Local governments may report cybersecurity incidents determined to be of severity level one or two and state agencies are required to report such incidents as soon as possible. State agencies and local governments report the incidents to the Cybersecurity Operations Center (CSOC) and Cybercrime Office; however, local governments are also required to report to the sheriff that has jurisdiction over the local government.

The bill specifies the information that must be reported in a cybersecurity or ransomware incident report by a state agency or local government. The incident report 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.
- If the reporting entity is a local government, a statement requesting or declining assistance from the CSOC, Cybercrime Office, or sheriff.

The bill requires the CSOC to notify the President of the Senate and the Speaker of the House of Representatives of any cybersecurity incident with a severity level of three, four, or five within 12 hours of receiving the state agency or local government incident report. The notification must include a high-level description of the incident and the likely effects. In addition, the CSOC must provide consolidated incident reports to the President of the Senate, Speaker of the House of Representatives, and Cybersecurity Advisory Council (CAC) on a quarterly basis. 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.

After-action Reports

The bill requires state agencies and local governments to submit an after-action report to Florida Digital Service (FLDS) within one week of the remediation of a cybersecurity or ransomware incident. The after-action report must summarize the incident, the incident's resolution, and any insights gained as a result of the incident. By December 1, 2022, the FLDS must establish guidelines and processes for submitting after-action reports.

Cybersecurity Training

The bill requires the FLDS to develop a basic and advanced cybersecurity training curriculum. All local government employees with access to the local government's network must complete the basic training curriculum, and local government technology professionals and employees with access to highly sensitive information must complete the advanced training curriculum. The

trainings must be completed by employees within 30 days of commencing employment and on an annual basis thereafter. The bill authorizes the FLDS to provide the cybersecurity trainings in collaboration with the Cybercrime Office, a private sector entity, or an institution of the State University System.

The bill requires the advanced cybersecurity training currently provided by the FLDS to state agency technology professionals to be provided on an annual basis and to be provided to employees with access to highly sensitive information. In addition, state agency heads must provide the basic cybersecurity training that is currently provided to agency employees on an annual basis.

The bill requires the advanced cybersecurity training curriculum provided to certain state and local government employees to include training on the identification of each cybersecurity incident severity level.

Local Government Cybersecurity Standards

The bill requires local governments to adopt cybersecurity standards that safeguard the local government's data, IT, and IT resources to ensure availability, confidentiality, and integrity. The standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute for Standards and Technology (NIST) cybersecurity framework. Counties with a population of 75,000 or more and municipalities with a population of 25,000 or more must adopt the standards by January 1, 2024. Counties with a population less than 75,000 and municipalities with a population less than 25,000 must adopt the standards by January 1, 2025. The bill requires each local government to notify the FLDS when it has adopted the standards.

Florida Cybersecurity Advisory Council

The bill provides that one of the purposes of the CAC is to advise local governments on cybersecurity, including cybersecurity threats, trends, and best practices. In addition, the bill requires the CAC to review information relating to cybersecurity and ransomware incidents reported by state agencies and local governments to determine commonalities and develop best practice recommendations for those entities. The CAC must recommend any additional information that should be reported by a local government to the FLDS as part of a cybersecurity or ransomware incident report.

Beginning December 1, 2022, and each December 1 thereafter, the CAC must prepare and submit a comprehensive report to the Governor, the President of the Senate, and the Speaker of the House of Representatives that includes data, trends, analysis, findings, and recommendations for state and local action regarding ransomware incidents. At a minimum, the report must include:

- Descriptive statistics, including the amount of ransom requested, duration of the incident, and overall monetary cost to taxpayers of the incident.
- A detailed statistical analysis of the circumstances that lead 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.
- Other recommendations to prevent ransomware incidents.
- The bill specifies that, for purposes of the CAC's charter, the term "state agency" includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

Ransomware Offense

The bill provides that a person who willfully, knowingly, and without authorization introduces a computer contaminant that gains unauthorized access to, encrypts, modifies, or otherwise renders unavailable data, programs, or supporting documentation residing or existing within a computer, computer system, computer network, or electronic device owned or operated by a government entity46 and demands a ransom to prevent the publication of or restore access to the data, programs, or supporting documentation or to otherwise remediate the impact of the computer contaminant commits a ransomware offense. The bill provides that a ransomware offense is punishable as a first degree felony. The bill further provides that an employee or contractor of a government entity, with access to the government entity's network, who willfully and knowingly aids or abets another in the commission of a ransomware offense against the government entity commits a felony of the first degree. In addition to any other penalties imposed, the convicted person must pay a fine equal to twice the amount demanded in the ransomware offense, the proceeds of which will be deposited into the General Revenue Fund.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

The county/municipality mandates provision of Art. VII, s. 18 of the Florida Constitution may apply because the bill places cybersecurity related requirements on local governments, including completing cybersecurity trainings, adopting cybersecurity standards, reporting ransomware and certain cybersecurity incidents, and submitting after-action reports; however, an exemption may apply if the costs related to those cybersecurity requirements are insignificant. An exception may apply because similarly situated entities are required to comply with the same cybersecurity requirements and the bill provides an important state interest determination. An exception may also apply because the General Appropriations Act provides estimated funds to cover the mandate.

The fiscal impact to the local governments is indeterminate as the number of impacted individuals is unknown.

The bill does not clearly define which entities within local government are covered by the requirements. For Fiscal Year 2020-2021, the total FTEs employed in Florida's 67

counties was reported as 158,685[59] and, for municipal governments, the total FTEs reported was 107,137.[60]

Expenditure of funds would be required of all counties and local governments similarly situated in that all counties and local governments would be required to comply in the same manner, which may remove the local mandate issue. Additionally, the fiscal impact to the local government may be insignificant depending on the format and type of training developed. Whether this requirement would meet the threshold to be considered a mandate is indeterminate.

The bill includes a statement that the act fulfills an important state interest.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

There is an indeterminate fiscal impact associated with providing the training to local government employees. The cost will be determined by the format and delivery of the training, as well as the number of individuals out of the total county or local government

[59] Office of Economic and Demographic Research, *Local Government Financial Reports, County Government Reports, 2020 Reporting Cycle Results*, pg. 12, *available at* http://edr.state.fl.us/Content/local-government/local-govt-reporting/2020CountyReport-DataSetwithMetrics.pdf (last visited Feb. 8, 2022).
[60] Office of Economic and Demographic Research, *Local Government Financial Reports, Municipal Government Reports, 2020 Reporting Cycle Results*, pg. 67, *available at* http://edr.state.fl.us/Content/local-government/local-govt-reporting/2020MunicipalReport-DataSetwithMetrics.pdf (last visited Feb. 8, 2022).

workforce that would be required to participate in either the new employee component or the annual training.

There may be long-term indeterminate savings in funds and resources to the state, local, or county governments if the cybersecurity trainings result in fewer cybersecurity attacks, reductions in the loss of data, or mitigation of third party computer breaches.

VI. Technical Deficiencies:

In describing the types of training to be delivered to local government employees, Section 2 of the bill does not define "persons with access to highly sensitive information" who would undergo additional training.

It is also unclear as to who is responsible for the delivery of the referenced cybersecurity training. Section (2) states that the Florida Digital Service may provide the training in collaboration with other defined entities. The statement implies that the Florida Digital Service is tasked with providing the training to applicable local government employees.

VII. Related Issues:

The bill requires that training be created and provided for certain employees of state and local government. The definition of local government is not provided. State statutes provide several provisions or definitions of "local government" depending on the context or legislative intent, which include or exclude other public institutions, such as schools, higher education entities, special districts, or councils.

VIII. Statutes Affected:

This bill substantially amends section 282.318 of the Florida Statutes.

This bill creates section 282.3185 of the Florida Statutes.

IX. Additional Information:

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

CS/CS by Appropriations on February 28, 2022:
The committee substitute:

- Requires state agencies and local government entities to report cybersecurity and ransomware incidents to the Cybersecurity Operations Center (CSOC) and the Cybercrime office of the Department of Law Enforcement;
- Defines the level of severity of a cybersecurity incident in accordance with the U.S. Department of Homeland Security's National Cyber Incident Response Plan;
- Requires the advanced cybersecurity training offered to specified state agency and local government employees to include training on the cybersecurity incident severity levels;

- Differentiates reporting requirements based on the level of severity of a cybersecurity incident;
- Requires the Legislature to only be notified of high severity level cybersecurity incidents;
- Requires the CSOC to provide the Legislature and Cybersecurity Advisory Council (CAC) with a consolidated incident report on a quarterly basis;
- Requires local government entities to adopt cybersecurity standards that align with the National Institute for Standards and Technology and to provide notification to the Florida Digital Service when such standards are adopted;
- Expands the purpose of the CAC to include advising local governments on cybersecurity and requires the CAC to examine reported cybersecurity and ransomware incidents to develop best practice recommendations;
- Requires the CAC to submit an annual comprehensive report regarding ransomware to the Governor and Legislature; and
- Establishes penalties and fines for certain ransomware offenses against a government entity.

CS by Military and Veterans Affairs, Space, and Domestic Security on February 8, 2022:

The Committee adopted a CS which:

- Modifies s. 282.318, F.S., to direct the Florida Digital Service (FDS) to provide cybersecurity training for all state agency technology employees and employees with access to highly sensitive information within the first 30 days of employment and then annually thereafter;
- Defines "local government" to mean any county or municipality";
- Creates s. 282.3185, F.S., and directs FDS to develop a basic and advanced cybersecurity training curriculum for local government employees with access to the local network or have access to highly sensitive information for completion within 30 days of employment and then annually thereafter; and
- Allows training to be provided by the Cybercrime Office of the FDLE, a private sector entity, or an institution of the state university system.

The CS includes a statement that the Legislature finds that the act fulfills an important state interest.

The effective date of the act is July 1, 2022.

B. Amendments:

None.