The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

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

Prepared By: The Professional Staff of the Committee on Appropriations

BILL:	CS/SB 1670
INTRODUCER:	Military and Veterans Affairs, Space, and Domestic Security Committee and Senator Hutson
SUBJECT:	Cybersecurity
DATE:	February 25, 2022
REVISED:	

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

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 1670 modifies cybersecurity training standards for state agencies and local governments by:

- Establishing training requirements for new state and local government employees relating to cybersecurity based on the employee's access level to a computer network;
- Requiring that such training be conducted within the first 30 days of employment and then annually thereafter;
- Directing the Florida Digital Service (FDS) to create a basic and advanced cybersecurity training curriculum for local governments; and
- Authorizing the FDS to provide the cybersecurity trainings in collaboration with the Cybercrime Office, a private sector entity, or an institution of the State University System.

The Legislature finds that this act fulfills an important state interest.

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 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]

---

[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).
[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*.

  - 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 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]

Florida Information Protection Act of 2014

The *Florida Information Protection Act of 2014*[12] 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

[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).
[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] Ch. 2014-189, Laws of Fla. (creating s. 501.171, F.S., effective July 1, 2014; Florida Information Protection Act).

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[13] and is fourth in the total amount of victim loss reported at $295 million for 2020.[14]

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. [15]

Information Technology Management

The Department of Management Services (DMS)[16] oversees information technology (IT)[17] governance and security for the executive branch of state government. The Florida Digital Service (FDS) within the DMS was established by the Legislature in 2020 to replace the Division of State Technology.[18] The head of the FDS is appointed by the Secretary of Management Services[19] and serves as the state chief information officer (CIO).[20]

The FDS 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.[21] Accordingly, the DMS through the FDS has the following powers, duties, and functions:

- Develop IT policy for the management of the state's IT resources.
- Develop an enterprise architecture.

---

[13] *Supra*, note 2.
[14] *Id.* at 24.
[15] 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).
[16] *See* s. 20.22, F.S.
[17] 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.
[18] Ch. 2020-161, Laws of Fla.
[19] The Secretary of Management Services serves as the head of Department of Management (DMS) and is appointed by the Governor, subject to confirmation by the Senate. Section 20.22(1), F.S.
[20] Section 282.0051(2)(a), F.S.
[21] Section 282.0051(1), F.S.

- Establish project management and oversight standards with which state agencies[22] 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.[23]
- 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.[24]

State Cybersecurity Act

The State Cybersecurity Act[25] requires the DMS and the heads of state agencies[26] to meet certain requirements to enhance the cybersecurity[27] of state agencies. Specifically, the DMS, acting through the FDS 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 National Institute for Standards and Technology (NIST) cybersecurity framework.
- Adopt rules to mitigate risk, support a security governance framework, and safeguard state agency digital assets, data,[28] information, and IT resources[29] 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.[30]

---

[22] "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.

[23] For the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services, Florida Digital Services (FDS) 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.

[24] Section 282.0051(1), F.S.

[25] Section 282.318, F.S.

[26] 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.

[27] "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.

[28] "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.

[29] "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.

[30] "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.

- 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.[31]

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.[32] In addition, the head of each state agency must:

- Establish an agency cybersecurity incident response team in consultation with FDS 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.
- 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. Except for sharing within the DMS, the cybercrimes unit of the FDLE, and certain agencies under the jurisdiction of the Governor and the Chief Inspector, these security plans are confidential and exempt from public review under s. 119.019(1), F.S.[33]
- Develop and periodically update written internal policies and procedures, including procedures for reporting cybersecurity incidents and breaches to the FDS 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 in written specifications for the solicitation, contracts, and service-level agreement of IT and IT resources and services meet or exceed

[31] Section 282.318(3), F.S.
[32] Section 282.318(4)(a), F.S
[33] Section 282.318(4)(d), F.S.

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 FDS for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents.[34]

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 State 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[35] 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.

[34] Section 282.318(4), F.S.
[35] 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.[36]

III. Effect of Proposed Changes:

Sections 1 and 2 require the Florida Digital Service (FDS) 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 the employees within 30 days of commencing employments and on an annual basis thereafter. The bill authorizes the FDS 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 FDS 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.

Section 3 provides a statement that the Legislature finds that the act fulfills an important state interest.

Section 4 provides an effective date of July 1, 2022.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

The bill requires the training of local government employees who have access to a local government network or access to highly sensitive information within the first 30 days of employment and then at annual intervals, thereafter. The fiscal impact to the local governments is indeterminate as the number of impacted individuals is unknown.

[36] 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).

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[37] and, for municipal governments, the total FTEs reported was 107,137.[38]

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.

[37] 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).
[38] 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).

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 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 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.