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 Military and Veterans Affairs, Space, and Domestic Security

BILL:	CS/SB 1670
INTRODUCER:	Committee on Military and Veterans Affairs, Space, and Domestic Security, and Senator Hutson
SUBJECT:	Cybersecurity
DATE:	February 8, 2022
REVISED:	

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

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; and
- Directing the Florida Digital Service (FDS) to create a basic cybersecurity curriculum for local governments.

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]which is used by malicious actors to encrypt files on devices, networks, or computer systems, rendering the files on those system 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 which 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:

> "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 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 February 4, 2022).
[2] Federal Bureau of Investigation, Internet Crime Complaint Center, 2020 Internet Crime Report, Business Email Compromise (BCE), p.10, available at https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited February 2, 2022).
[3] The Federal Bureau of Investigation (FBI) defines ransomware as malicious software, or malware that encrypts files on a victim's computer which prevents an individual from accessing his or her computer files, systems, or networks and demands that an individual pay a ransom for the return of the information or data or to provide a key to decrypt the files. See FBI Public Service Announcement, "High Impact Ransomware Attacks Threaten U.S. Businesses and Organizations," Alert Number I-100219-PSA (October 2, 2019), available at *https://www.ic3.gov/Media/Y2019/PSA191002* (last visited February 4, 2022).
[4] *Supra*, note 2.
[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 February 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 end the cyber-attack.[10]

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

- 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 cyber-attack 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 every February 1st with

---

[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 January 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 January 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 January 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 January 23, 2022).

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

the Legislature a report identifying any governmental entities which 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 civilly 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 $295,032,829 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]

Florida Digital Service

The Florida Digital Service (FDS) was created as a division under s. 20.22, F.S., within the Department of Management Service (DMS), during the 2020 Legislative Session and its powers and duties were established under s. 282.0051. F.S, specifically. The FDS is charged with proposing innovative solutions that securely modernize state government, including technology and information services which achieve value through digital transformation and interoperability, and which fully support the cloud-first policy.[16]

The FDS is also responsible for the training of all state agency technology professionals. The training may be conducted in coordination with the FDLE, a private sector entity, or an institution of the state university system.[17] Operation and maintenance of a Cybersecurity Operations Center (Center) by the FDS was included in the 2020 legislation. The Center must be led by the state chief information security officer and must serve as a clearinghouse for threat information, which must be primarily virtually and be coordinated with FDLE.

Each state agency head is required to designate an information security manager to administer the cybersecurity program of his or her respective state agency and to establish a cybersecurity

[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 January 24, 2022).
[16] Section 282.0051(1), F.S.
[17] Section 282.318(3)(h), F.S.

response team.[18] Each state agency develops and maintains a three-year security plan which is updated and assessed every three years.[19] Except for sharing within the DMS, the cybercrimes unit of 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.[20]

Unfunded Local Government Mandates

An unfunded mandate on local government is defined in Florida's Constitution as a general law which require 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, Section 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 2/3 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[21] 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.

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.

[18] Section 282.318(4)(a) and (b), F.S.
[19] Section 282.318(4)(c), F.S.
[20] Section 282.318(4)(d), F.S.
[21] 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.

Mandates can be exempted in certain circumstances such as if they 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.[22]

III. Effect of Proposed Changes:

Sections 1 and 2 – Amending sections 282.318, F.S. (Cybersecurity) and creating section 282.3185, F.S., (Local government cybersecurity).

CS/SB 1670 requires state and local government agencies to conduct cybersecurity trainings within the first 30 days of employment and then annually thereafter as follows:

Florida Digital Service (FDS) will:
- Develop a basic cybersecurity practices training curriculum; and
- Develop an advanced cybersecurity training as required under s. 282.318(3)(g).

Local government agencies, defined as counties and municipalities, shall:
- Train state agency technology professionals; and
- Employees with access to highly sensitive information access.

A local government may provide the required cybersecurity training in collaboration with the Cybersecurity Crimes Office of the Department of Law Enforcement, a private sector entity, or an institution of the state university system.

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 the 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 unclear as the number of impacted individuals is unknown.

[22] 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 January 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 6,101.29[23] and for municipal governments, the total FTEs reported was 101,776.75.[24]

Expenditure of the 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.

CS/SB 1670 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.

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

C. Government Sector Impact:

There may be an indeterminate fiscal impact to local and county governments for the cost of the cybersecurity training. It is unknown what format the training may be or how many individuals out of the total county or local government workforce 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.

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 252.318 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.)

Recommended CS by Committee on 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.