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:	SB 1670
INTRODUCER:	Senator Hutson
SUBJECT:	Cybersecurity
DATE:	February 7, 2022
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Lloyd	Caldwell	MS	**Pre-meeting**
2.			AEG	
3.			AP	

I. Summary:

SB 1670 modifies and establishes standards which enhance state agency's and local government's abilities to respond to cybersecurity and ransomware incidents including:

- Establishing reporting requirements for local governments and hospitals for cybersecurity and ransomware incidents to the Florida Digital Service (FDS), State Watch Office, Executive Office of the Governor, and local law enforcement agencies within designated timeframes;
- Creating definitions for "ransomware" and "local government";
- Requiring each local government adopt cybersecurity standards for all information and operational technology in accordance with national guidelines by January 1, 2024;
- Establishing training requirements for local government employees relating to cybersecurity based on the employee's access level to be conducted at the beginning of employment and then annually;
- Directing the Florida Digital Service (FDS) to create a checklist for use by local governments prior to payment of any ransom; and
- Requiring local governments to communicate any ransom demands to the FDS and local law enforcement agencies prior to any payment.

The bill establishes fines and penalties for unauthorized users of computers, computer networks, computer systems, and electronic devices. Collected fines will be shared among the FDS and the local law enforcement agencies and any private or public entities or individuals who aided in the conviction of the defendant.

The bill includes a non-recurring appropriation of $1 million to the FDS to be disbursed to the local governments for training. Other indeterminate, negative fiscal impacts to the local governments for implementation, reporting of breaches, ongoing training costs, and any negative

business reputation from public acknowledgement of data breaches are anticipated and similar negative impact to a hospital's business reputation would be expected for any reporting hospital facilities.

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

II. Present Situation:

General Background – Data Security

Ransomware[1] is a form of malware[2]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,[3] 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."[4]

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.[5] This represents a 69 percent increase in total complaints from 2019.

---

[1] Ransomware is not defined in federal or Florida statutes. 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 athttps://www.ic3.gov/Media/Y2019/PSA191002 (last visited February 4, 2022).

[2] "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).

[3] 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).

[4] 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).

[5] *Supra,* note 6.

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.[6]
    - 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.[7]
    - 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.[8]
- JBS, the world's largest meat processing plant, was hit by a ransomware attack in June 2021:[9]
    - The plant is responsible for supplying one quarter of America's beef.[10]
    - 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.[11]

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.

What is Cybersecurity?

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

---

[6] 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.*
[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).
[9] *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).
[10] *Id.*
[11] *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).

increases in both cyberattacks and particularly, ransomware attacks, according to statistics from the University of West Florida's Center for Cybersecurity.[12]

In the President's May 12, 2021, Executive Order (Order), he declared that incremental improvements in America's current cybersecurity systems were no longer enough to ensure protection of the nation's current information technology infrastructure.[13] The Order included requirements for specific contract language for reporting on cybersecurity incidences and incorporating revised standards for federal contract language which impacts entities that hold or collect data on behalf of the federal government which would include contracts between the federal and state government. [14]

The Order also standardizes the federal government's response to cybersecurity vulnerabilities and incidents through creation of a "playbook" or a standard set of operational procedures to be used for planning and conducting a cybersecurity vulnerability and incident response activity. The playbook is required to:

- Include appropriate *National Institute of Standards and Technology (NIST)* standards.
- Be used by all Federal Civilian Executive Branch agencies (FCEB);[15]
- Articulate progress and completion through all phases of an incident response, while allowing flexibility;
- Apply to agencies with cybersecurity vulnerability or incident response procedures that deviate from the playbook;
- Be reviewed and updated annually by the Director of the CISA, in consultation with the Director of the National Security Agency;
- Ensure comprehensiveness of incident response activities and build confidence that unauthorized cyber actors no longer have access to FCEB Information Systems;
- Establish, consistent with applicable law, a requirement that the Director of CISA review and validate FCEB agencies' incident response and remediation results upon an agency's completion of its incident response; and
- Include a common lexicon to be shared among all agencies using the playbook.

National Institute for Standards and Technology Framework (NIST)

The *National Institute for Standards and Technology (NIST)* was founded in 1901 by Congress to address competitiveness issues the United States faced at the time as the country's measurement infrastructure lagged behind that of other industrial countries.[16] The *NIST* develops measurement standards and tools for new technologies, including weights and measurements,

---

[12] 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).
[13] Executive Order Improving the Nation's Cybersecurity, 86 Fed. Reg. 26633, 26633 (E.O. 14028, proposed May 12, 2021) available at https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf (last visited January 21, 2022).
[14] *Id*.
[15] Federal Civilian Executive Branch Agencies (FCEB) means all agencies except for the Department of Defense and agencies in the intelligence community. *See* Executive Order Improving the Nation's Cybersecurity, 86 Fed. Reg. 26633, 26633 (E.O. 14028, proposed May 12, 2021) available at https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf (last visited January 21, 2022).
[16] National Institute for Standards and Technology, *About Us/About NIST,* available at *https://www.nist.gov/about-nist* (last visited February 2, 2022).

cybersecurity and privacy, communications, health and biological systems, and physical infrastructure and resilience.

Section 531.39, F.S., provides that weights and measures that are traceable to the United States prototype standards supplied by the Federal Government, or approved as being satisfactory by the *NIST*, shall be the state primary standards of weights and measures, and shall be maintained in such calibration as prescribed by the *NIST.* The Department of Agriculture and Consumer Services is required to establish regulations regarding technical requirements for commercial weighing and measuring devices that conform to those adopted by the *NIST* to the extent possible.[17]

Federal Privacy Standards

Federal Privacy Act of 1974

The *Federal Privacy Act of 1974*[18] *(Privacy Act)* governs the collection, use, and dissemination of a "record"[19] about an "individual"[20] maintained by federal agencies in a "system of records."[21] Affected agencies must maintain only such information as is relevant and necessary to accomplish the agency's purpose[22] and to ensure that no record is disclosed to any person or any other agency, except by the written request or prior consent of the individual, unless the request meets one of the statute's twelve specific exceptions.[23] The *Privacy Act* also applies to systems of records created by government contractors, but does not apply to private databases.[24] Additionally, the *Privacy Act* requires a written agreement between a source agency[25] and a recipient agency[26] or a non-federal agency[27] which includes any state or local government for computer matching programs. Records contained in the system of records will not be shared or disclosed except pursuant to a written agreement which complies with federal requirements.[28] An example of a program which currently conducts state and federal data matching under such agreements is the Florida Medicaid program.

Health Data Privacy and Security

Cybersecurity is also affected by boundaries established through federal health information privacy and security laws, regulations, and standards such as the *Health Insurance Portability*

[17] Section 531.40, F.S.
[18] 5 U.S.C. § 552(a).
[19] 5 U.S.C. § 552(a)(4).
[20] 5 U.S.C. § 552(a)(2).
[21] 5 U.S.C. § 552(a)(5).
[22] 5 U.S.C. § 552(e).
[23] 5 U.S.C. §552(b). Records may be disclosed without an individual's written consent for reasons which include, but are not limited to: research or statistical purposes, law enforcement activity, the record has historical value, compelling circumstances which may affect the health or safety of an individual, to either House of Congress for issues relating to matters within their jurisdiction, pursuant to a court order, or to a consumer reporting agency.
[24] 5 U.S.C. § 552(m).
[25] 5 U.S.C. § 552(a)(11).
[26] 5 U.S.C. § 552(a)(9).
[27] 5 U.S.C. § 552(a)(10).
[28] 5 U.S.C. § 552(o).

and Accountability Act of 1996 (HIPAA)[29] and the subsequent legislation to include additional entities known as business associates[30] under the *Health Information Technology for Economic and Clinical Health Act*[31] *(HITECH).* Under these laws and associated regulations, individual health information held by covered entities[32] and their business associates can only be shared with certain individuals or entities for specific purposes and individuals have the right to ask that their information not be shared with certain individuals or entities and to ask that errors in their medical records be corrected.[33] The *HIPAA* and *HITECH Acts* establish standards for the administrative, technical, and physical safety of the data held by covered entities and business associates. Covered entities must ensure the protection of data and safeguard it from any intention or unintentional use or disclosure that violates those standards.[34]

HIPAA Breach Notification Rule

When there has been a breach of protected health information, the covered entity is required to notify those individuals that have been impacted.[35] Covered entities must provide individual notices to those impacted by first class mail or electronic mail if that method has been requested by the individual, customer service through a toll-free number for 90 days after the notice, and posted information on a website. When more than 500 individuals are impacted, a mass media alert and notice to the Secretary of Health and Human Services is required for HIPAA covered entities or to the Federal Trade Commission (FTC) for non-HIPAA covered entities must be made without unreasonable delay, but in no case later than 60 calendar days from discovery.[36] Covered under entities under HHS and FTC reporting requirements must maintain breach logs for data breaches of less than 500 individuals for annual submissions, as appropriate.[37]

---

[29] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. Law No. 104-191(August 21, 1996).
[30] For HIPAA purposes, a business associate is considered an entity who helps a covered entity carry out its health care activities and functions. The covered entity must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with HIPAA. *See* CMS.GOV, HIPAA and Administrative Simplification, *Are you a covered entity?*, available at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity (last visited February 2, 2022).
[31] Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. No. 115-5, s. 13400 (February 17, 2009), available at https://www.congress.gov/111/plaws/publ5/PLAW-111publ5.pdf (last visited January 24, 2022).
[32] For HIPAA purposes, a covered entity is a health plan or health insurance company (includes health maintenance organizations, employer sponsored health plans, and government programs that pay for health care like Medicare, Medicaid, and military and veterans' health program), clearinghouses (organizations that process nonstandard health information to conform to the standards for data content or format, or vice versa, on behalf of other organizations), or providers who submit HIPAA transactions such health care claims. *See* CMS.GOV, HIPAA and Administration Simplification, *Are you a covered entity?* available at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity (last visited February 2, 2022).
[33] Department of Health and Human Services, Office of Civil Rights, *Your Health Information Privacy Rights*, available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf (last visited February 2, 2022).
[34] 45 C.F.R. § 164.530(c).
[35] 45 C.F.R. §§164.400-414.
[36] Federal Trade Commission, *Health Breach Notification Rule*, 16 C.F.R. Part 318 (2009).
[37] U.S. Department of Health and Human Services, *Submitting a Notice of a Breach to the Secretary*, available at https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last visited January 25, 2022). Both the electronic form for notifying the Secretary and a link to a historical list of breaches greater than 500 is found on this page.

Federal Duty to Report Incidents

Federal Information Security Modernization Act of 2014 (FISMA)

Organizations are also required, in accordance with federal law, to create and operate formal incidence response capabilities, specific to cybersecurity. The *Federal Information Security Modernization Act of 2014 (FISMA)* is the principal law governing the federal government's information security program. The *FISMA* requires the head of each federal agency to be responsible for information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.[38]

These guidelines and protections are applicable to both the federal agencies and any contractors or organizations that work on behalf of a federal agency. Breaches of personally identifiable information must be reported within one hour of discovery or detection unless a delay is necessary for law enforcement, national security purposes, or agency needs.[39]

Florida Information Protection Act of 2014

The Florida Information Protection Act of 2014[40] 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 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.

[38] 44 U.S.C. §3554(a)(1)(A).
[39] Gina Stevens, *Federal Information Security and Data Breach Notification Laws,* Congressional Research Service (January 28, 2010), pp. 7-8, available at https://sgp.fas.org/crs/secrecy/RL34120.pdf (last visited February 2, 2022).
[40] Ch. 2014-189, Laws of Fla. (creating s. 501.171, F.S., effective July 1, 2014; Florida Information Protection Act).

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[41] and is fourth in the total amount of victim loss reported at $295,032,829 for 2020.[42]

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 in the chart below.

Examples of Florida Attorney General Data Breach Settlements – Multiple State Agreements[43]			
Year of Breach	**Settlement Year**	**Entity**	**Description**
2012-20	2019	Yahoo!	Multiple State Settlement; 3.5 billion accounts affected by 4-year data breach.
2014	2020	Anthem	Multiple State Settlement; malware attack through phishing email; impacted 78 million Americans, including 1.5 million Floridians.
2017	2020	Equifax	Multi-State Settlement; affected half of US population (147 million people impacted); hackers accessed system for 76 days.
2020	2020	Sabre Hospitality Solutions	Multi-State Settlement; hospitality booking group – hacker accessed credit card data for 18 months
2020	2020	Home Depot	Multi-State Settlement; breach of customer credit card data.
2020	2021	Community Health Sys	Multi-State Settlement; TN-Based health care system for breach of patient data.

Florida Digital Service

The Florida Digital Service (FDS) was created as a division under s. 20.22, F.S., within the 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.[44]

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. [45] 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, which is required to be primarily virtual, and must serve as a clearinghouse for threat information and be coordinated with FDLE.

---

[41] *Supra,* note 6.
[42] *Id.* at 24.
[43] 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).
[44] Section 282.0051(1), F.S.
[45] Section 282.318(3)(h), F.S.

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 response team.[46] Each state agency develops and maintains a three-year security plan which is updated and assessed every three years.[47] 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.[48]

Florida Cybersecurity Task Force

HB 5301 created the Florida Cybersecurity Task Force (Task Force)[49] which was charged with reviewing and recommending improvements to the state's cybersecurity infrastructure, governance, and operations. Prior to HB 5301, the responsibilities for the state's cybersecurity was decentralized and fragmented across several state agencies including the AST and the Florida Department of Law Enforcement (FDLE) without requirements for coordination, emergency management planning, IT security plans, or continuity of business plans. The Task Force convened in October 2019 and was replaced by the Florida Cybersecurity Advisory Council July 1, 2021.

Florida Cybersecurity Advisory Council

The Florida Cybersecurity Advisory Council (council), an advisory council as defined in s. 20.03(7), F.S.,[50] was created within the DMS, succeeded the Florida Cybersecurity Task Force and was established in CS/CS/HB 1297 during the 2021 Regular Legislative Session. The council's purpose is to assist state agencies and the FDS in protecting their information technology resources and implementing the best cybersecurity practices.

The maximum 19-member council includes the Lieutenant Governor and representatives from the FDS office, DEM, FDLE, Public Service Commission, universities, critical infrastructure sector, cybersecurity or software engineering sector (public or private sector), and emerging technologies sector. The Secretary of the DMS, or his or her designee, serves as an ex-officio member of the council. The enabling legislation directs the council to submit annual recommendations to the President of the Senate and the Speaker of the House of Representatives on cybersecurity beginning June 30, 2022.

[46] Section 282.318(4)(a) and (b), F.S.
[47] Section 282.318(4)(c), F.S.
[48] Section 282.318(4)(d), F.S.
[49] The Florida Cybersecurity Task Force was a task force created as defined under s. 20.03(8), F.S., and operated adjunct to the Department of Management Services, to review and assess the state's cybersecurity infrastructure, governance, and operations. The Division of State Technology of the DMS provided the administrative and staffing support for the task force. A "committee" or "task force" under s. 20.03(8), F.S., means an advisory body created without a specific statutory enactment for a time period not to exceed one year or created by a specific statutory enactment for a time not to exceed three years and appointed to study a specific problem and recommend a solution or policy alternative with respect to that problem. Its existence terminates upon the completion of its assignment.
[50] "Council" or "Advisory Council" means an advisory body created by a specific statutory enactment and appointed to function on a continuing basis for the study of the problems arising in a specified function or program area of state government and to provide recommendations and policy alternatives.

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 to be 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 needed to be sufficient to fund 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[51] 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.

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.[52]

[51] 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.
[52] 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*

Hospitals

Hospitals are licensed in the state under chapter 395, F.S., and the general licensure provisions of part II, of chapter 408, F.S., by the Agency for Health Care Administration (AHCA). Hospitals offer a range of health care services which are defined specifically under s. 395.002(13), F.S. Additional regulatory standards for hospital licensure are provided under Rule 59A-3., F.A.C., and are administered through the AHCA.

III. Effect of Proposed Changes:

Section 1 amends s. 252.351, F.S., to add to the list of certain incidences by which an identified political subdivision must notify the Division of Emergency Management (DEM) of any attacks on a computer or network of a local government, as defined in s. 215.89(2)(c), F.S., or a hospital, as defined in s. 395.002(13), including incidences of ransomware and data breaches. The definition of a local government is specific to the definition found under s. 215.89(2)(c), F.S., which limits the definition to mean a "municipality, county, water management district, special district, or any other entity created by a local government." The definition specifically does not include an "educational entity"[53] or an "entity of higher education"[54] which are defined separately in this same section of law. The limiting term "political subdivision" has been stricken from the short title for this section as the addition of the new paragraph (l) could mean that an educational or hospital entity are not also political subdivisions thereby making the existing short title no longer a workable title.

Section 2 creates s. 282.3185, F.S., establishing duties and responsibilities for local governments, as defined in s. 215.89(2)(c), F.S., adopting cybersecurity technology and operational standards and requiring local governments to:

- Comply with the *NIST Framework* as appropriate to the size of their organization.
- Adopt standards which include multi-factor authentication.
- Report adopted standards to the Florida Digital Service (FDS).
- Conduct vulnerability testing no less than every two years.
- Train certain local employees relating to phishing and digital hygiene training, as specified by FDS, at time of hiring and then annually.
- Provide intensive training to local government technology professionals with highly sensitive access, at time of hiring and then annually.
- Report any cybersecurity and ransomware incidents to the State Watch Office, FDS, Executive Office of the Governor, FDLE, and local law enforcement within 12 hours of discovery.
- Submit summaries of cybersecurity reports and ransomware events to the Council.
- Communicate with FDS and local law enforcement agencies before any payment by local government of ransom or extortion demands.

---

http://www.leg.state.fl.us/data/Publications/2000/Senate/reports/interim_reports/pdf/00-24ca.pdf (last visited January 26, 2022).

[53] An "educational entity" means a school district or an entity created by a school district" under s. 215.89(2)(d), F.S.

[54] An "institution of higher education" means a state university, a state or Florida College System institution, or an entity created by a state university or state or Florida College System Institution" under s. 215.89(2)(e), F.S.

- Consider ransomware checklist created by FDS before paying a ransom.

The bill also directs the State Chief Information Officer and Council to advise the Governor directly on cybersecurity and ransomware events. State agencies, like local governments, would also be required to report any cybersecurity or ransomware incidents.

Section 3 amends s. 815.06, F.S., to add a definition for "ransomware" to the chapter on computer-related crimes and the section relating to offenses against users of computers, computer systems, computer networks, and electronic devices. The term "ransomware" is defined to mean a computer contaminant or lock placed or introduced without authorization into a computer, computer system, computer network, or electronic device which does any of the following:

- Restricts access by an authorized person to the computer, computer system, computer network, or electronic device or to any data held by the computer, computer system, computer network, or electronic device under circumstances in which the person responsible for the placement or introduction of the computer contaminant or lock demands payment of money or other consideration to:
  - Remove the computer contaminant or lock;
  - Restore access to the computer, computer system, computer network, electronic device, or data; or
  - Otherwise remediate the impact of the computer contaminate or lock; or
- Transforms data held by the computer, computer system, or computer network, or electronic device into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

The definition for "ransomware" is limited and excludes situations which include:

- Threats to release the information or data to the public unless a ransom is paid;
- Where authentication may be required to upgrade or access purchased content; or
- Access is blocked to subscription content in the case of non-payment for that access.

A person who places ransomware in a computer, computer system, computer network, or an electronic device under this section will commit a felony of the first degree, punishable as provided under s. 775.082. F.S., (imprisonment) or s. 775.084, F.S., (enhanced penalties or mandatory minimum sentencing) and shall be assessed a fine equal to twice the amount of ransom demanded in the attack or the maximum fine provided under s. 775.083, F.S., which is greater. Fines collected under this act are split between the FDS and the law enforcement agencies and private entities or individuals who may have aided in the apprehension and conviction of defendant.

An employee or a contractor of the government of this state or a local government who knowingly places ransomware or introduces a computer contaminant on a computer, computer system, computer network, or electronic device commits a third degree felony, punishable as provided in s. 770.082, F.S., (imprisonment), s. 775.083, F.S., (fines), or s. 775.084, F.S., (enhanced penalties or mandatory minimum sentencing).

Section 4 provides a non-recurring appropriation for the 2022-2023 fiscal year of $1 million to the FDS which is to be disbursed to the local governments for the required training under s. 282.3185(3), F.S.

Section 5 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, as defined under s. 215.89(2)(c), F.S., who have access to a local government network when he or she begins employment and then at annual intervals, thereafter. The training must address, at a minimum, phishing and digital hygiene and be based on requirements established by the FDS and delivered virtually. Additionally, for those employees with access to highly sensitive information, which is not defined or further described, these employees must undergo what is vaguely described as intensive cybersecurity training.
SB 1670 provides a non-recurring appropriation of $1 million to FDS for disbursement to the counties to pay for the required training. If dispersed equally among all 67 counties, each county would receive slightly less than $15,000.

It is unclear how much the computer training would cost as the bill speaks of two types of training. One is a virtual platform to be conducted certain times of the year, and the second, would be an intensive training for cybersecurity professionals. 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 by the FDS. Whether this requirement would meet the threshold to be considered a mandate is indeterminate.

The bill does not currently include a statement that the training and any expenditure of funds by the local government fulfills an important state interest. The Legislature could also meet the other part of the mandate by passing the bill by a two-thirds vote of the membership in both chambers.

B. Public Records/Open Meetings Issues:

The bill has a linked public records exemption bill, SB 1694, to make confidential and exempt from s. 119.017(1), F.S., and s. 24(a), Art. I of the State Constitution, certain information relating to records in a criminal investigation that could reveal means or methods that may allow unauthorized access to computers, computer systems, computer networks, or electronic devices or to any data held by those same computers, computer systems, computer networks, or electronic devices in which the person who is responsible for the contaminant or lock demands payment of money or other consideration as provided in s. 815.06, F.S. While not addressed in SB 1670, these issues will be addressed in the linked bill.

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:

The bill requires hospitals, as defined in s. 395.002(13), F.S., to be included in the mandatory reporting of incidences relating to attacks on computers or networks. The fiscal impact to private hospital facilities is indeterminate as there is both the actual cost of identifying and reporting the breadth of the attack as well as the business cost to the facility in its potential loss of reputation in public acknowledgement of a data breach.

C. Government Sector Impact:

In addition to incurring the same costs as those of noted by the private facilities above, local government entities that meet the statutory definition used in SB 1670 would also be required to provide several layers of cybersecurity training to their employees. The cost of this training is unknown as the FDS is the entity which will determine the content of the training. The bill does not provide those parameters.

The bill includes a non-recurring fiscal allocation of state funds of $1 million; however, it is not clear how those funds will be allocated amongst the counties or municipalities. The funds are appropriated to the FDS, but the bill indicates that the funds are for the local governments' costs of training.

VI. Technical Deficiencies:

Florida licenses both public and private hospitals through the AHCA. For both initial and ongoing licensure, reporting provisions are found in chapter 395 and chapter 408, F.S. The duty for a hospital to report ransomware attacks and data breaches may belong more appropriately in one of those statutory chapters to align with functions already regulated by the AHCA. Hospitals already have a duty to report data breaches under the *HIPAA* and placement of these additional responsibilities in one of these other statutory sections may complement existing requirements.

In describing the types of training to be delivered to local government employees, the bill, in lines 99 through 101, does not define "persons with access to highly sensitive information" who would undergo the also undefined "intensive cybersecurity training."

VII. Related Issues:

The bill provides a cross reference for the definition of "local government" which excludes schools and higher education entities. In the past two years, at least two Florida school boards paid a significant ransom through their insurer to unlock the district's computer systems, including one of the nation's and Florida's largest school districts, Broward School District, who was hacked by a criminal gang which demanded $40 million or they would erase files and post personal information online.[55] In December 2020, the federal *Cybersecurity Infrastructure Security Agency* reported that K-12 schools accounted for 57 percent of all ransomware attacks in August and September, but only 28 percent of all attacks for January through July.[56] Under the bill, school districts would not be covered by the requirement to report ransomware attacks or to notify the FDS prior to payment of any ransom. There are several other definitions within the Florida Statutes that define local government, local governmental entities, or public agencies which would include school districts, schools, or higher education.

SB 1670 includes new deliverables and responsibilities for the FDS and the Council, including some which are time sensitive; however, very few include deadlines or timelines for completion. To ensure accountability and timely completion, these new milestones may need timeframes for completion by the designated parties.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 252.351 and 815.06.

This bill creates section 282.3185 of the Florida Statutes.

IX. Additional Information:

A. Committee Substitute – Statement of Changes:

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

None.

B. Amendments:

None.

[55] Terry Spencer, et al, *Large Florida school district hit by ransomware attack* (April 1, 2021), ABCNEWS.GO.COM, available at https://abcnews.go.com/US/wireStory/large-florida-school-district-hit-ransomware-attack-76818911 (last visited January 27, 2022).
[56] *Id.*