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 Judiciary

BILL:	SB 658
INTRODUCER:	Senator DiCeglie
SUBJECT:	Cybersecurity Incident Liability
DATE:	January 26, 2024
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Bond	Cibula	JU	**Pre-meeting**
2.			GO	
3.			RC	

I. Summary:

SB 658 provides that a county or municipality that has adopted cybersecurity protocols established by the Department of Management Services and has timely notified the state and the local sheriff of a serious incident related to cybersecurity is not liable for damages related to the incident.

The bill also provides that a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity or third-party agent that acquires, maintains, stores, or uses personal information is not liable in connection with a cybersecurity incident if the entity substantially complies with the Florida Information Protection Act (FIPA), adopts standards and guidelines in substantial alignment with the current version of any of 6 national standards listed, adopts standards and guidelines that substantially align with all of the 4 federal laws that may apply to the entity (including HIPAA and Gramm-Leach-Bliley), and updates its standards and guidelines within 1 year of an update to the prevailing standard.

The protections afforded by the bill are an affirmative defense where the defendant entity has the burden of proof on applicability.

The bill is effective upon becoming law.

II. Present Situation:

Cybersecurity is the practice of protecting computer systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal

business processes.[1] This bill addresses liability of local governments and private entities regarding liability for a cybersecurity incident. One commentator summed up the issue:

> Hardly a week goes by nowadays without headlines of yet another incident of corporate hacking or cybersecurity theft. Companies that electronically store sensitive information are facing the ever-changing challenge of guarding against unauthorized access to and misuse of such digital data. Critical computer-based assets increasingly have come under siege, and sophisticated hackers seem to be outpacing prophylactic measures designed to thwart their advance. As a result, digital data breaches have become almost commonplace today not only for multinational companies, but also for small and midsize companies. In short, cybersecurity has emerged as more than just an IT challenge--it is now a business and legal imperative.[2]

Current Cybersecurity Standards

Local Government Cybersecurity Act

Section 282.3185, F.S., is known as the Local Government Cybersecurity Act. The act first requires counties and municipalities to adopt cybersecurity standards that safeguard the local government's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity.[3] The standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[4] A local government must notify Florida Digital Service[5] (FLDS) that it has adopted standards to conform as soon as possible after adoption.[6] The deadline for adoption of standards was January 1, 2024, for counties having a population of 75,000 or more and cities having a population of 25,000 or more. All other counties and municipalities have until January 1, 2025, to comply.

The act classifies cybersecurity incidents or ransomware incidents into 5 categories based on the severity of the incident:

- Level 5 is an emergency-level incident within the specified jurisdiction that poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local government security; or the lives of the country's, state's, or local government's residents.

---

[1] Cisco.com, *What is Cybersecurity?* https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#:~:text=Cybersecurity%20is%20the%20practice%20of,or%20interrupting%20normal%20business%20processes (last visited Jan. 26, 2024).
[2] Hooker & Pill, *You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, Fla. B.J., 90-7, p. 30 (July/August 2016).
[3] Section 282.3185(4)(a), F.S.
[4] *Id*.
[5] The Florida Digital Service is an office within the Department of Management Services 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 the cloud-first policy. Section 282.0051(1), F.S.
[6] Section 282.3185(4)(d), F.S.

- Level 4 is a severe-level incident that is likely to result in a significant impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; or civil liberties.
- Level 3 is a high-level incident that is likely to result in a demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.
- Level 2 is a medium-level incident that may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.
- Level 1 is a low-level incident that is unlikely to impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.[7]

The act requires a county or municipality to provide notification of a level 3, 4, or 5 cybersecurity incident or ransomware incident to the Cybersecurity Operations Center, Cybercrime Office of the Department of Law Enforcement, and to the sheriff who has jurisdiction over the local government. The notification must include, at a minimum, the following information:

- A summary of the facts surrounding the cybersecurity incident or ransomware incident.
- The date on which the local government most recently backed up its data; the physical location of the backup, if the backup was affected; and if the backup was created using cloud computing.
- The types of data compromised by the cybersecurity incident or ransomware incident.
- The estimated fiscal impact of the cybersecurity incident or ransomware incident.
- In the case of a ransomware incident, the details of the ransom demanded.
- A statement requesting or declining assistance from the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction over the local government.[8]

The report of a level 3, 4, or 5 ransomware incident or cybersecurity incident must be sent as soon as possible but no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident.[9] Reporting a level 1 or 2 incident is optional and there is no deadline.[10]

A local government must submit to the Florida Digital Service, within 1 week after the remediation of a cybersecurity incident or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident.[11]

Florida Information Protection Act (FIPA)[12]

FIPA is a data security statute that requires governmental entities, specific business entities, and any third-party agent that holds or processes personal information on behalf of these entities to

[7] Section 282.318(3)(c)9.a., F.S.
[8] Section 282.3185(5)(a), F.S.
[9] Section 282.3185(5)(b)1., F.S.
[10] Section 282.3185(5)(c), F.S.
[11] Section 282.3185(6), F.S.
[12] Section 501.171, F.S.; Chapter 2014-189, Laws of Fla.

take "reasonable measures to protect and secure" a consumer's personal information.[13] FIPA defines "personal information" as:

- Online account information, such as security questions and answers, email addresses, and passwords; and
- An individual's first name or first initial and last name, in combination with any one or more of the following information regarding him or her:
  - A social security number;
  - A driver license or similar identity verification number issued on a government document;
  - A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
  - Medical history information or health insurance identification numbers; or
  - An individual's health insurance identification numbers.[14]

Personal information does not include information:

- About an individual that a federal, state, or local governmental entity has made publicly available; or
- That is encrypted, secured, or modified to remove elements that personally identify an individual or that otherwise renders the information unusable.[15]

FIPA requires covered business entities[16] that have suffered a data breach to notify affected individuals of the breach as expeditiously as possible, and no later than 30 days after discovering the breach.[17] However, the notice to affected individuals may be delayed at the request of a law enforcement agency, and notice is not required if the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed.[18]

If more than 500 individuals were affected by the breach, notice of the breach must also be given to the Department of Legal Affairs (DLA) as expeditiously as possible and no more than 30 days later.[19] If more than 1,000 individuals were affected by the breach, notice must also be given to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.[20] The Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p), provides the timing, distribution, and content of the notices to consumers.

FIPA does not provide a private cause of action, but authorizes the DLA to file a civil action against covered entities under Florida's Unfair and Deceptive Trade Practices Act (FDUTPA).[21]

---

[13] Section 501.171(2), F.S.
[14] Section 501.171(1)(g)1., F.S.; OAG *supra* note 41.
[15] Section 501.171(1)(g)2., F.S.
[16] A "covered entity" is a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. Section 501.171(1)(b), F.S.
[17] Section 501.171(4)(a), F.S.
[18] Section 501.171(4)(c), F.S.
[19] Section 501.171(3), F.S.
[20] Section 501.171(5), F.S.
[21] Sections 501.171(9) and (10), F.S.

In addition to the remedies provided for under FDUTPA, a covered entity that fails to notify the DLA, or an individual whose personal information was accessed, of the data breach is liable for a civil penalty of $1,000 per day for the first 30 days of any violation; $50,000 for each subsequent 30-day period of violation; and up to $500,000 for any violation that continues more than 180 days. These civil penalties apply per breach, not per individual affected by the breach.[22]

Cybersecurity Standards

There are various recognized cybersecurity standards and regulations. The ones referenced in the bill are:

Cybersecurity Standards	
Standard	**Description**
National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity	This publication contains multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. While intended for use in critical infrastructure, much of the standards are usable by any organization to improve security and resilience.[23]
NIST special publication 800-171	Provides recommended requirements for protecting the confidentiality of controlled unclassified information. If a manufacturer is part of a Department of Defense, General Services Administration, NASA, or other state or federal agency supply chain then they must comply with these security requirements.[24]
NIST special publications 800-53 and 800-53A	A category of security and privacy controls. Covers the steps in the Risk Management Framework that address security controls for federal information systems.[25]
The Federal Risk and Authorization Management Program security assessment framework	Organization established by the General Services Administration (a Federal Government Program) that provides U.S. federal agencies, state agencies, and their vendors with a standardized set of best practices to assess, adopt, and monitor the use of cloud-based technology services under the Federal Information Security Management Act (FISMA).[26]

[22] Section 501.171(9)(b), F.S.
[23] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited Jan. 24, 2024).
[24] NIST, *What is the NIST SP 800-171 and Who Needs to Follow It?*, https://www.nist.gov/blogs/manufacturing-innovation-blog/what-nist-sp-800-171-and-who-needs-follow-it-0#:~:text=NIST%20SP%20800-171%20is%20a%20NIST%20Special%20Publication,protecting%20the%20confidentiality%20of%20controlled%20unclassified%20information%20%28CUI%29 (last visited Jan. 24, 2024).
[25] NIST, *Selecting Security and Privacy Controls: Choosing the Right Approach*, https://www.nist.gov/blogs/cybersecurity-insights/selecting-security-and-privacy-controls-choosing-right-approach (last visited Jan. 25, 2024).
[26] Reciprocity, *How State and Local Agencies Can Use FedRAMP*, https://reciprocity.com/how-state-and-local-agencies-can-use-fedramp/#:~:text=The%20Federal%20Risk%20and%20Authorization%20Management%20Program%20%28FedRAMP%29,cloud%20products%20offered%20by%20cloud%20service%20providers%20%28CSPs%29 (last visited Jan. 25, 2024).

Cybersecurity Standards	
Standard	**Description**
CIS Critical Security Controls	The Center for Internet Security Critical Security Controls (CIS) are a prescriptive and simplified set of best practices for strengthening cybersecurity for different organizations. CIS was created in response to extreme data losses experienced by organizations in the U.S. defense industrial base.[27]
The International Organization for Standardization/International Electrotechnical Commission 27000 – series family of standards	ISO/IEC 27001 (ISO) enables organizations of all sectors to manage security of financial information, intellectual property, employee data and information entrusted by third parties. ISO has auditors and is an international standard. There are 804 technical committees and subcommittees concerned with such standards of development.[28]
Health Insurance Portability and Accountability Act of 1996	Commonly referred to as HIPAA, this federal law requires the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.[29]
Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA)	The GLBA governs the treatment of nonpublic personal information about consumers, which information is held by financial institutions.[30]
Federal Information Security Modernization Act of 2014, Pub. L. No. 113-2 (FISMA 2014)	FISMA 2014 codifies the Department of Homeland Security's role in administering the implementation of information security policies for federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting OMB in developing those policies.[31]

[27] CIS Security, *CIS Critical Security Controls*, https://www.cisecurity.org/controls (last visited Jan 24, 2024).
[28] ITGovernance, *ISO 27001, The International Security Standard*, https://www.itgovernanceusa.com/iso27001#:~:text=ISO%2027001%20is%20a%20globally%20recognized%20information%20security,trusted%20benchmark.%20Protect%20your%20data%2C%20wherever%20it%20lives (last visited Mar. 29, 2023).
[29] Centers for Disease Control and Prevention, *Health Insurance Portability and Accountability Act of 1996 (HIPPA)*, https://www.cdc.gov/phlp/publications/topic/hipaa.html (last visited Jan. 26, 2024).
[30] Federal Deposit Insurance Corporation, *Gramm-Leach-Bliley Act* (Apr. 2021), https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/8/viii-1-1.pdf.
[31] Cybersecurity & Infrastructure Security Agency, *Federal Information Security Modernization Act*, https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act#:~:text=Overview,OMB%20in%20developing%20those%20policies (last visited Jan. 26, 2024).

Cybersecurity Standards	
Standard	**Description**
Health Information Technology for Economic and Clinical Health Act requirements	The American Recovery & Reinvestment Act of 2009 established the Health Information Technology for Economic Clinical Health Act, which requires that Centers for Medicare and Medicaid Services provide incentive payments under Medicare and Medicaid to "Meaningful Users" of Electronic Health Records.[32]

Tort Liability and Negligence -- In General

A tort is a civil legal action to recover damages for a loss, injury, or death due to the negligence of another. According to the Florida Standard Jury Instructions, negligence means "doing something that a reasonably careful person would not do" in a similar situation or "failing to do something that a reasonably careful person would do" in a similar situation.[33] To establish liability, the plaintiff must prove four elements:

- Duty – That the defendant owed a duty, or obligation, of care to the plaintiff;
- Breach – That the defendant breached that duty by not conforming to the standard required;
- Causation – That the breach of the duty was the legal cause of the plaintiff's injury; and
- Damages – That the plaintiff suffered actual harm or loss.

While the Legislature has the power to create, define and modify the laws governing tort actions, much of the tort law is defined by the common law. As to data information and cybersecurity, torts in this area are relatively new and not well defined.[34]

III. Effect of Proposed Changes:

The bill provides that a county or municipality that substantially complies with the requirements of the Local Government Cybersecurity Act in s. 282.3185, F.S., is not liable in connection with a cybersecurity incident. A local government complies with the act by adopting certain cybersecurity standards and timely notifying the state and the local sheriff of a serious breach. It further provides that a county's or municipality's failure to substantially implement a cybersecurity program that complies with s. 282.3185, F.S., does not constitute evidence of negligence or negligence per se.

The bill provides that a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity or third-party agent that acquires, maintains, stores, or uses personal information is not liable in connection with a cybersecurity incident if the entity

[32] Centers for Medicare & Medicaid Services, Health Information Technology for Economic Critical (HITECH) Audits, https://www.cms.gov/medicare/audits-compliance/part-a-cost-report/health-information-technology-economic-and-clinical-health-hitech-audits#:~:text=The%20American%20Recovery%20%26%20Reinvestment%20Act,Users%E2%80%9D%20of%20Electronic%20Health%20Records, (last visited Jan. 26, 2024).
[33] Fla. Std. Jury Instr. Civil 401.3, *Negligence*.
[34] Hooker & Pill, *You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, Fla. B.J., 90-7, p. 30 (July/August 2016).

substantially complies with the Florida Information Protection Act (FIPA), and substantially aligns its operations with the current version of any of the following:

- NIST Framework for Improving Critical Infrastructure Cybersecurity.
- NIST special publication 800-171.
- NIST special publications 800-53 and 800-53A.
- Federal Risk and Authorization Management program security assessment framework;
- CIS Critical Security Controls.
- International Organization for Standardization/International Electrotechnical Commission 27000-series family of standards.

Additionally, if the sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity or third-party agent is regulated by the state or federal government pursuant to any of the following laws, its cybersecurity program must also substantially align to the current version of any of the following that apply in order to receive the liability protections of the bill:

- Health Insurance Portability and Accountability Act of 1996.
- Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA).
- Federal Information Security Modernization Act of 2014, Pub. L. No. 113-2 (FISMA 2014).
- Health Information Technology for Economic and Clinical Health Act requirements.

A sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity or third-party agent that has substantially complied with the requirements of this bill and who has thereby attained the protections against liability must adopt revised conforming frameworks or standards within 1 year after the latest publication date stated in the revision should 2 or more of its pertinent frameworks or standards be updated.

The bill specifies that it does not establish a private cause of action.

The protections afforded by the bill are an affirmative defense, the defendant has the burden of proof to show substantial compliance with a standard, law, or regulation. In examining the scale and scope of substantial alignment with a standard, law, or regulation, the finder of fact must consider the following criteria:

- Size and complexity of the covered entity.
- Nature and scope of the covered entity's activities.
- Sensitivity of the information that the business protects.

The bill is effective upon becoming law.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

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:

Private businesses may enjoy lower cyber liability insurance premiums as a result of their shield from liability created by the bill, but may face increased costs for compliance with standards that may not currently be required.

C. Government Sector Impact:

None.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill creates section 768.401 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.