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 Governmental Oversight and Accountability

BILL:	CS/SB 692
INTRODUCER:	Governmental Oversight and Accountability Committee and Senator Leek
SUBJECT:	Cybersecurity Standards and Liability
DATE:	January 27, 2026 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Harmsen	McVaney	GO	**Fav/CS**
2.			JU	
3.			AP	

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 692 provides protections from liability for a cybersecurity incident to counties, municipalities, political subdivisions, private entities, and their third-party agents. To avail themselves of this protection, the local government or private entity must have implemented policies that substantially comply or align with specific cybersecurity standards or frameworks. A local government must also have adopted a disaster recovery plan for cybersecurity incidents and multi-factor authentication. A private entity and their third-party agent must additionally comply with applicable state and federal laws, such as the Florida Information Protection Act, which requires consumer notification of a breach, and applicable privacy laws.

A local government is afforded a total limitation on liability in connection with a cybersecurity incident if it meets the bill's cybersecurity requirements. A covered entity or a third-party agent is instead granted a presumption against liability in a class action that results from a cybersecurity incident. In either case, the initial burden of proof shifts to the defendant to establish substantial compliance with the bill's cybersecurity requirements.

The bill also provides that local governments may only impose the same or lower cybersecurity standard or process as it applies to itself to its information technology commodity or service vendors, unless otherwise required by state or federal law, or industry-specific requirements which apply to regulated sectors.

There is no impact expected on state revenues and expenditures. Local governments may experience an indeterminate impact on its expenditures related to decreased liability and costs for cyber liability insurance. See Section V.

The bill takes effect upon becoming a law but provides for applicability to any putative class action filed before, on, or after the effective date.

II. Present Situation:

Cybersecurity is the protection of networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.[1] Cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.[2] This bill addresses liability of local governments and private entities regarding liability for a cybersecurity incident.

Current Cybersecurity Standards

Local Government Cybersecurity Act

Section 282.3185, F.S., is known as the Local Government Cybersecurity Act (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; all counties and municipalities should have adopted at least their first version of standards by January 1, 2025.[6]

The act classifies cybersecurity or ransomware incidents into five 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, state, or local government's residents.

---

[1] U.S. Cybersecurity and Infrastructure Security Agency, *What is Cybersecurity?* (Feb. 1, 2021), https://www.cisa.gov/news-events/news/what-cybersecurity (last visited Jan. 21, 2026).
[2] 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. 20, 2026).
[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)(c)-(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 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 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]

The 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,

[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.

to take "reasonable measures to protect and secure" a consumer's personal information.[13] The 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]

The FIPA requires covered entities, including governmental 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.

The 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.
[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

The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce.[23] The Cybersecurity Enhancement Act of 2014 expanded NIST's role, directing it to support the development of cybersecurity risk frameworks. Under this mandate, NIST created a prioritized, flexible, and cost-effective framework to help critical infrastructure owners and operators identify, assess, and manage cyber risks. This framework formalized NIST's earlier work under Executive Order 13636 (2013), "Improving Critical Infrastructure Cybersecurity," and continues to guide future cybersecurity initiatives.[24] While originally designed for critical infrastructure, the framework has since evolved into a widely used cybersecurity resource across all sectors, including government, businesses, academia, and nonprofits. It is designed to be flexible, scalable, and adaptable, making it useful for organizations regardless of size, industry, or cybersecurity maturity level. Unlike prescriptive regulations, the framework provides broad, outcome-based guidance, allowing organizations to tailor their cybersecurity strategies to their unique risks, resources, and operational goals. It can be used as a standalone framework or integrated with existing cybersecurity programs. Organizations may adopt it to assess current cybersecurity postures, identify gaps, and establish a roadmap for continuous risk management. As such, there are a variety of ways to use the framework; the decision about how to apply it is left to the implementing organization.[25]

Other guidelines and frameworks referenced in the bill are:

Cybersecurity Standards and Applicable Privacy Laws	
Standard	**Description**
NIST Cybersecurity Framework 2.0	A publication that contains multiple approaches to cybersecurity by assembling standards, guidelines, and practices. While intended for use in critical infrastructure, many of the standards are useful to any organization to improve security and resilience.

[22] Section 501.171(9)(b), F.S.
[23] NIST, *NIST History*, https://www.nist.gov/history (last visited Jan. 21, 2026).
[24] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* at v-vi (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited Jan. 21, 2026).
[25] NIST, *The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0*, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (last visited Jan. 20, 2026).

Cybersecurity Standards and Applicable Privacy Laws	
Standard	**Description**
NIST special publication 800-171	A publication that 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.[26]
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.[27] These guidelines are primarily used by federal agencies and government contractors to comply with federal security mandates, but are also widely adopted by private sector organizations for cybersecurity risk management.[28]
The Federal Risk and Authorization Management Program (FedRAMP) security assessment framework	An organization established by the General Services Administration (a Federal Government Program) that provides government agencies and their vendors, as well as private cloud service providers 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).[29]
Center for Internet Security Critical Security Controls (CIS)	A prescriptive and simplified set of best practices for strengthening cybersecurity for different organizations.[30]

[26] 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. 21, 2026).
[27] 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 Feb. 1, 2024).
[28] See NIST Special Publication 800-53 Revision 5, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf and NIST Special Publication 800-53A Revision 5, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf (last visited Jan. 21, 2026).
[29] *See* U.S. General Services Administration, *FedRAMP*, https://www.gsa.gov/technology/government-it-initiatives/fedramp and FedRAMP, *Overview*, https://www.fedramp.gov/20x/ (last visited Jan. 21, 2026).
[30] CIS Security, *CIS Critical Security Controls*, https://www.cisecurity.org/controls (last visited Jan. 21, 2026); DOT Security, *Explaining the Critical Security Controls (CSC) by the Center for Internet Security* (Oct. 3, 2024), https://dotsecurity.com/insights/blog-explaining-cis-critical-security-controls (last visited Jan. 21, 2026).

Cybersecurity Standards and Applicable Privacy Laws	
Standard	**Description**
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.[31]
HITRUST Common Security Framework (CSF)	A compliance framework primarily used in healthcare, but adaptable to other industries that consolidates multiple cybersecurity and privacy standards to help organizations streamline their security programs.[32]
Service Organization Control Type 2 Framework (SOC 2)	A framework developed by the American Institute of Certified Public Accountants, it ensures that third-party service providers securely store and process client data. Compliance is based on five trust service principles: security, privacy, availability, confidentiality, and processing integrity.[33]
Secure Controls Framework	A meta-framework incorporating various cybersecurity and data privacy controls to help organizations build secure and compliant programs.[34]
Health Insurance Portability and Accountability Act of 1996	Commonly referred to as HIPAA, a federal law that requires the creation of national standards to protect

[31] 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 Jan. 21, 2026).
[32] HITrust Alliance, *Introduction to the HITRUST CSF, Version 11.7.0* at 5 (Dec. 2025), https://hitrustalliance.net/hubfs/CSF/CSF%20v11.7/Introduction%20to%20HITRUST%20CSF%20v11.7.0.pdf (last visited Jan. 21, 2026); Richard Rieben, LINFORD & CO, *Understanding the HITRUST CSF: A Guide for Beginners* (Mar. 15, 2023), https://linfordco.com/blog/hitrust-csf-framework/ (last visited Jan. 21, 2026).
[33] Secureframe, *What is SOC2?*, https://secureframe.com/hub/soc-2/what-is-soc-2 (last visited Jan. 21, 2026).
[34] *See* Secure Controls Framework, *FAQ: What is the SCF?*, https://securecontrolsframework.com/faq/faq (last visited Jan. 21, 2026).

Cybersecurity Standards and Applicable Privacy Laws	
Standard	**Description**
	sensitive patient health information from being disclosed without the patient's consent or knowledge.[35]
Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA)	A law that governs the treatment of nonpublic personal information about consumers, which information is held by financial institutions.[36]
Federal Information Security Modernization Act of 2014, Pub. L. No. 113-2 (FISMA 2014)	A law that 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.[37]
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.[38]

[35] Centers for Disease Control and Prevention, *Health Insurance Portability and Accountability Act of 1996 (HIPPA)*, https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html?CDC_AAref_Val=https://www.cdc.gov/phlp/publications/topic/hipaa.html (last visited Jan. 21, 2026).
[36] 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 (last visited Jan. 21, 2026).
[37] 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. 21, 2026). *See also*, U.S. Chief Information Officers Council, *Policy Overview*, https://www.cio.gov/policies-and-priorities/FISMA/ (last visited Jan. 21, 2026).
[38] 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. 21, 2026).

Cybersecurity Standards and Applicable Privacy Laws	
Standard	**Description**
Criminal Justice Information Services (CJIS) Security Policy	Minimum security requirements, guidelines, and agreements to protect the sources, transmission, and storage of criminal justice information (located on the FBI's CJIS system) held by both criminal justice and non-criminal justice agencies.[39]

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.[40] 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.

In Florida, negligence cases follow a modified comparative negligence rule, which means that a plaintiff can only recover damages if they are 50 percent or less at fault for their own harm.[41] Plaintiffs found to be more than 50 percent responsible are barred from recovering any damages. When awarding damages, the jury assigns a percentage of fault to each party, and any compensation awarded is reduced accordingly.

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 (court-made) law. As to data information and cybersecurity, torts in this area are relatively new and not well defined.[42]

Burden of Proof and Legal Presumptions

The burden of proof refers to the obligation to establish a material fact in a legal dispute.[43] Generally, the party asserting a fact bears the burden.[44] In civil cases, the plaintiff must prove allegations in the complaint, while in criminal cases, the prosecution must prove the defendant's guilt. Conversely, a defendant raising an affirmative defense—whether in a civil or criminal

[39] Federal Bureau of Investigation, *Criminal Justice Information Services Security Policy* (Jun. 1, 2020), https://www.fbi.gov/file-repository/cjis/cjis_security_policy_v5-9_20200601.pdf/view (last visited Jan. 21, 2026)
[40] Fla. Std. Jury Instr. Civil 401.3, *Negligence*.
[41] Section 768.81(6), F.S. This comparative negligence rule does not apply to an action for damages for personal injury or wrongful death arising out of medical negligence pursuant to ch. 766, F.S. Additionally, the comparative negligence standard does not apply to any action brought to recover economic damages from pollution, an intentional tort, or where joint and several liability is specifically provided for, as in chs. 403, 517, 542, and 895, F.S.
[42] 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).
[43] Black's Law Dictionary (12th ed. 2024), burden of proof.
[44] *See Berg v. Bridle Path Homeowners Ass'n, Inc.*, 809 So.2d 32 (Fla. 4th DCA 2002).

case—must prove the elements of that defense.[45] In some instances, statutory or common law presumptions shift the burden of proof to the opposing party unless sufficiently rebutted.[46]

Sovereign Immunity

Sovereign immunity is a legal doctrine that prevents the government from being sued without its consent.[47] The State Constitution allows the Legislature to waive this immunity,[48] and the Florida Statutes permit tort claims against the state, its agencies, and subdivisions for damages caused by negligence of government employees acting within the scope of their employment.[49] However, liability exists only when a private individual would be held liable for the same conduct and applies specifically to injury or loss of property, personal injury, or death.[50] The law also limits tort recovery against a governmental entity to $200,000 per person and $300,000 per incident. Although a court may enter a judgement exceeding these caps, a claimant generally cannot collect more than the statutory limits unless the Legislature approves a claim bill granting additional compensation.[51] Additionally, government employees, officers, and agents are generally immune from personal liability for actions taken within the scope of employment, unless they act in bad faith, with malicious purpose, or with wanton and willful disregard for human rights, safety, or property.[52] A government entity is not liable for actions taken by an employee outside the scope of employment or for actions committed by an employee with bad faith, malicious intent, or reckless disregard for others' rights or safety.[53]

Class Action Lawsuits

A class action lawsuit allows one or more plaintiffs to sue on behalf of a larger group, or "class," that has suffered similar harm. This procedural device enables courts to efficiently manage lawsuits that would be otherwise unmanageable if each affected individual had to file separately. Class actions also help protect defendants from inconsistent judgments and allow plaintiffs to share litigation costs.[54]

A class action lawsuit is filed when a plaintiff submits a complaint seeking to represent a class of similarly affected individuals. However, at this stage, the case is not yet a certified class action—it is considered a putative class action until the court determines whether to grant class certification. If the court denies certification, the lawsuit continues only for the named plaintiffs and does not proceed as a class action. If certified, the judgement or settlement in the case is

[45] An affirmative defense is a defendant's assertion of facts that, if true, defeat the plaintiff's or prosecution's claim, even if the allegations in the complaint are accurate. The defendant bears the burden of proving an affirmative defense, which may include duress in civil cases or insanity and self-defense in criminal cases. Black's Law Dictionary (12th ed. 2024), defense.
[46] *See* Black's Law Dictionary (12th ed. 2024), presumption; Cornell Law School, Presumption (last visited January 14, 2026).
[47] Miles McCann, NATIONAL ASSOCIATION OF ATTORNEYS GENERAL, *State Sovereign Immunity* (Nov. 11, 20217), https://www.naag.org/attorney-general-journal/state-sovereign-immunity/ (last visited Jan. 21, 2026).
[48] Art. X, s. 13, FLA. CONST.
[49] Section 768.28(5), F.S.
[50] *Id*.
[51] Section 768.28, F.S.
[52] Section 768.28(9), F.S.
[53] *Id*.
[54] Legal Information Institute, Cornell Law School, *Class Action*, https://www.law.cornell.edu/wex/class_action (last visited Jan. 21, 2026).

binding on all class members, who are generally prohibited from filing individual lawsuits raising the same claim.[55]

III. Effect of Proposed Changes:

Section 1 amends s. 282.3185, F.S., to prohibit a local government, which includes counties and municipalities,[56] from imposing a higher cybersecurity standard or process than it has adopted for itself on its vendors that provide information technology commodities or services, except where a higher standard is otherwise required by state or federal law, or an industry-specific requirement that applies to a regulated sector.

This provision applies to contracts entered into or amended by the local government on or after July 1, 2026, with a "vendor," which for purposes of this section, is defined as a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity.

Section 2 creates s. 768.401, F.S., to provide that a county, municipality, or other political subdivision[57] is not liable *in any action* for a cybersecurity incident if it has implemented (1) one or more policies that substantially comply with one of the cybersecurity standards or frameworks specified in the bill or a similar standard or framework; (2) a disaster recovery[58] plan for cybersecurity incidents; and (3) multi-factor authentication (MFA). A local government is generally covered by sovereign immunity under s. 768.28, F.S., which would limit the local government's liability to $200,000 per person, or up to $300,000 per incident in a negligence action that resulted in injury or the loss of property. This provision would reduce the local government's liability to $0 per incident, if it meets the requirements provided by the bill.

The cybersecurity standards and frameworks specified in statute are:

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0;
- NIST special publication 800-171;
- NIST special publications 800-53 and 800-53A;
- The Federal Risk and Authorization Management Program Security Assessment Framework;
- The Center for Internet Security (CIS) Critical Security Controls;
- The International Organization for Standardization/International Electrotechnical Commission 27000 series (ISO/IEC 27000) family of standards;
- HITRUST Common Security Framework (CSF);
- Service Organization Control Type 2 Framework (SOC 2);
- Secure Controls Framework; or
- Other similar industry frameworks or standards.

---

[55] Fla. R. Civ. P. 1.220. For discussion of the rule and its meaning, *see* Ervin A. Gonzalez and Raymond W. Valori, *Considerations in Class Actions*, 72 FLA. B. J. 78 (1998), https://www.floridabar.org/the-florida-bar-journal/considerations-in-class-certification/ (last visited Jan. 21, 2026).

[56] *See* s. 282.3185(2), F.S., which defines a "local government" for purposes the section as a county or municipality.

[57] A "political subdivision" includes counties, cities, towns, villages, special tax school districts, special road and bridge districts, bridge districts, and all other districts in Florida. Section 1.01, F.S.

[58] For purposes of s. 768.401, F.S., created by this bill, "disaster recovery" means the process, policies, procedures, and infrastructure related to preparing for and implementing recovery or continuation of ana agency's vital technology infrastructure after a natural or human-induced disaster.

MFA is a security measure that requires users to verify their identity using at least two factors before accessing an account. According to industry experts, enabling MFA can prevent 99 percent of automated hacking attacks.[59]

Additionally, the bill provides that a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity ("covered entity"), or their third-party agent that acquires, maintains, stores, processes, or uses personal information has a presumption against liability *in a class action* filed in connection with a cybersecurity incident if the entity substantially complies with the Florida Information Protection Act (FIPA), and has implemented a policy that substantially complies with the cybersecurity standards or frameworks listed above. However, if the covered entity is regulated by state or federal governments, their cybersecurity program may comply with the following laws, as appropriate, instead of the cybersecurity standards or frameworks:

- 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.
- Criminal Justice Information Services Security Policy.
- Other similar requirements mandated by state or federal laws or regulations.

A covered entity or third-party agent that has substantially complied with the requirements of this bill and thereby attained the liability protections set forth in this bill must adopt revised conforming frameworks or standards within one year of their latest published update.

A covered entity or third-party agent may demonstrate their effective implementation of a cybersecurity program in compliance with the bill by providing documentation or other evidence of an assessment, conducted either by an internal auditor or a third-party.

The local government, covered entity, or third-party agent's failure to implement a cybersecurity program that complies with s. 768.401, F.S., does not in and of itself constitute evidence of negligence or negligence *per se*, and according to the bill, may not be used as evidence of fault under any other theory of liability.

Whether a local government, a covered entity, or a third-party agent, in order to avail itself of the liability protections afforded by this bill, the defendant in a civil action relating to a cybersecurity incident has the burden of proof to show substantial compliance with the bill's requirements, codified as s. 768.401, F.S. However, this affirmative defense does not apply to individual civil actions filed against a covered entity or third-party agent, whereas it does for local governments.

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

A putative class action is one in which the class has not yet been certified by a court. The bill specifies that it applies to a putative class action that was filed before, on, or after the effective

[59] *See* National Cybersecurity Alliance, *What is Multifactor Authentication and Why Should You Use It?* (Jan. 17, 2025), https://www.staysafeonline.org/articles/multi-factor-authentication?fob=EbZrACZuzBt4U2Sw (last visited Jan. 21, 2026).

date of the act. Although this has the effect of adding a defense for a party against whom a lawsuit has already been filed, it is likely a procedural impact rather than a substantive one. Because the affirmative defense created by the bill applies only to class action lawsuits, not to individual actions, the individual may still pursue his or her vested, substantive interest in courts without the defendant's ability to argue a newly-created affirmative defense.[60]

The bill takes effect upon becoming a law.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

Not applicable. The bill does not require municipalities or counties to spend funds, reduce the authority of municipalities or counties to raise revenue, or reduce the percentage of state tax shared with municipalities and counties.

B. Public Records/Open Meetings Issues:

None Identified.

C. Trust Funds Restrictions:

None identified.

D. State Tax or Fee Increases:

None identified.

E. Other Constitutional Issues:

None identified.

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. Those same businesses, however, may face increased costs to comply with new standards required in the bill.

[60] *See*, *China Agritech v. Resh*, 584 US 732, 735 (2018) (A court's denial of a class certification leaves intact a putative class member's option to pursue an individual suit.) *See also*, *Am. Pipe & Const. Co. v. Utah's,* 414 U.S. 538, 94 S. Ct. 756, 38 L. Ed. 2d 713 (1974).

C. Government Sector Impact:

Local governments may enjoy lower cyber liability insurance premiums as a result of the protection from liability in this bill.

Courts may see a reduction in class action cases filed as a result of cybersecurity incidents. An individual may still pursue his or her claim on an individual basis, but the attorneys fees and costs associated with an individual claim may deter such claims.

VI. Technical Deficiencies:

While the bill provides methods to demonstrate compliance, but the term remains undefined. This may result in disparate findings by courts based on similar facts.

The bill provides that an entity's implementation of specified policies creates a presumption against liability in certain actions. However, the bill does not specify at what point before the action is instituted that the entity must have implemented the cybersecurity program. This means that certain entities may assert the presumption against liability for incidents that happened prior to the entity enacting the new cybersecurity standards. The sponsor may wish to specify that the entity must have adopted the specified policies prior to the incident which gave rise to the claim.

VII. Related Issues:

None identified.

VIII. Statutes Affected:

This bill substantially amends section 282.3185 and creates s. 768.401 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 Governmental Oversight and Accountability on January 26, 2026:
Requires local governments to impose the same, or a lesser cybersecurity standard or process as it has adopted for itself on a vendor that provides IT commodities or services, unless otherwise required by state or federal law, or industry-specific requirements apply to regulated sectors. This provision applies to contract the local government enters into or amends on or after July 1, 2026.

B. Amendments:

None.