FLORIDA HOUSE OF REPRESENTATIVES
BILL ANALYSIS

This bill analysis was prepared by nonpartisan committee staff and does not constitute an official statement of legislative intent.

BILL #: CS/HB 1183	**COMPANION BILL:** SB 1576 (DiCeglie)
TITLE: Cybersecurity Incident Liability	**LINKED BILLS:** None
SPONSOR(S): Giallombardo	**RELATED BILLS:** None

Committee References

Information Technology Budget & Policy 14 Y, 2 N, As CS	➤ Civil Justice & Claims	➤ State Affairs

SUMMARY

Effect of the Bill:

The bill provides liability protection for local governments (i.e., counties, municipalities, and political subdivisions) and private entities in connection with cybersecurity incidents. Local governments are shielded from liability from all lawsuits related to a cybersecurity incident if they substantially comply with cybersecurity standards or align with cybersecurity frameworks, maintain disaster recovery plans, and implements multi-factor authentication.

The bill provides private entities and third-party agents a presumption against liability in class action lawsuits related to cybersecurity incidents if they have a cybersecurity program that substantially complies with Florida's data breach notification laws, substantially complies with cybersecurity standards or aligns with cybersecurity frameworks, maintains disaster recovery plans, and implements multi-factor authentication. Additionally, entities regulated under federal or state law may qualify by demonstrating substantial compliance with applicable cybersecurity requirements.

Fiscal or Economic Impact:

The bill may have a positive fiscal impact on the state, local governments, and the private sector by reducing liability for local governments and providing a presumption against liability in class action lawsuits for private entities in connection with cybersecurity incidents, thereby lowering legal expenses and financial liabilities. Additionally, the state court system may experience reduced strain on resources due to a decrease in litigation. However, the overall fiscal impact remains indeterminate, as potential saving depend on the number of lawsuits that would have otherwise been filed, how frequently the presumption is invoked and the outcomes of related litigation, and whether affected individuals choose to pursue individual claims instead of class actions.

JUMP TO SUMMARY ANALYSIS RELEVANT INFORMATION BILL HISTORY

ANALYSIS

EFFECT OF THE BILL:

The bill provides liability protections—in connection with a cybersecurity incident—for local governments (i.e., counties, municipalities, and other political subdivisions) that implement policies that substantially comply with specified cybersecurity standards or frameworks (or similar standards or frameworks), maintain disaster recovery plans, and implement multi-factor authentication (MFA). (Section 1)

For private entities and third-party agents[1] that acquire, maintain, store, process, or use personal information, the bill provides a presumption against liability in class action lawsuits—in connection with a cybersecurity incident—if they have a cyber security program that substantially complies with Florida's data breach notification laws, implements policies that substantially comply with specified cybersecurity standards and frameworks (or similar standards or frameworks), maintain disaster recovery plans, and implement MFA. If a covered entity or third-party

[1] A "third-party agent" is an entity contracted to maintain, store, or process personal information on behalf of a "covered entity", which is a private entity.

agent is regulated by federal or state data protection or security laws, substantial compliance with those laws is considered sufficient to qualify for liability protections. (Section 1)

To demonstrate compliance, covered entities and third-party agents may provide documentation or other evidence of assessments—conducted internally or by a third-party. The bill also requires organizations to update their cybersecurity programs within one year of any revisions to relevant frameworks or laws in order to retain liability protection. (Section 1)

The bill does not create a private cause of action. Additionally, failure to implement a compliant cybersecurity program does not constitute negligence per se and cannot be used as evidence of negligence or fault under any other theory of liability against a private entity, third-party agent, or local government. If a local government, covered entity, or third-party agent is sued in connection with a cybersecurity incident, the burden of proof is on the defendant to establish substantial compliance with the cybersecurity requirements outlined in the bill. (Section 1)

The bill applies to any suit filed on or after the bill's effective date and to any putative class action not certified on or before the effective date of this act. (Section 2)

The effective date of the bill is upon becoming a law. (Section 3)

FISCAL OR ECONOMIC IMPACT:

STATE GOVERNMENT:

The bill may result in a positive fiscal impact on the state by creating a presumption against liability for private entities in class action lawsuits related to cybersecurity incidents. However, if a significant number of potential class members choose to file individual lawsuits instead, the expected cost savings may be reduced or negated. Additionally, shielding local governments from liability may decrease the number of lawsuits filed against them, potentially reducing the caseload for state courts. The overall fiscal impact on the state court system is indeterminate at this time, as it depends on how affect individuals respond to the bill's liability framework and how many cases would have otherwise been brought against local governments absent the bill's protections.

LOCAL GOVERNMENT:

The bill may have a positive fiscal impact on local governments by reducing legal expenses and financial liabilities related to cybersecurity incidents due to the liability shield. The fiscal impact is indeterminate at this time, as it depends on the number of cybersecurity incidents for which local governments would have otherwise been liable but for the protections under the bill.

PRIVATE SECTOR:

The bill may have a positive fiscal impact on private businesses. By providing a presumption against liability in class action lawsuits against businesses and third-party agents that handle personal information in connection with a cybersecurity incident, the bill may reduce legal expenses and financial liabilities. However, businesses and third-party agents seeking liability presumptions must substantially comply with Florida's data breach notification laws and implement industry cybersecurity frameworks and best practices, which could require additional cybersecurity investment depending on their current security posture. The overall fiscal impact is indeterminate at this time, as the extent of cost savings from litigation outcomes will vary based on how often the presumption is successfully invoked and the nature of claims brought against covered entities.

Additionally, the bill may have an indeterminate positive fiscal impact on private individuals by incentivizing businesses, third-party agents, and local governments to adopt certain cybersecurity measures. These actions could help protect data (e.g., taxpayer and consumer personal information), information technology (IT), and IT resources from unauthorized access. If these entities enhance their cybersecurity posture, it may reduce the frequency and impact of cyberattacks on private individuals in the state.

RELEVANT INFORMATION

SUBJECT OVERVIEW:

Legislative Authority Over Causes of Action

The Florida Constitution guarantees the right to access to the courts, ensuring that they "shall be open to every person for redress of any injury."[2] However, this right is not absolute. In *Kluger v. White*,[3] the Florida Supreme Court ruled that while the Legislature has the power to modify or restrict legal causes of action, it cannot eliminate a "traditional and long-standing" cause of action arbitrarily or on a mere legislative whim. The Court outlined specific conditions under which the Legislature may lawfully limit or abolish a cause of action. First, it may reduce a cause of action so long as it does not completely eliminate the right to sue.[4] Second, it may abolish a cause of action that is neither historically rooted in common law nor established by statute before the adoption of the Florida Constitution's Declaration of Rights.[5] Lastly, the Legislature may abolish a cause of action if it provides a reasonable alternative remedy[6] or demonstrates an "overpowering public necessity" that cannot be addressed through any other means.[7] This framework ensures that legislative action altering legal remedies remains consistent with constitutional protects while allowing for necessary policy changes.

Tort Liability

A *tort* is a civil wrong for which the law provides a remedy. Tort law is designed to fairly compensate individuals who have been harmed by another's wrongful actions—whether intentional, reckless, or negligent—through civil legal process. An effective tort system serves several key functions:

- Ensures a fair and equitable forum for resolving disputes.
- Compensates individuals who have suffered legitimate harm.
- Allocates financial responsibility to those at fault.
- Encourages responsible behavior to prevent future harm.
- Deters wrongful conduct by imposing legal consequences.[8]

Negligence in Tort Law

Negligence is a legal concept in tort law that applies to actions that cause harm unintentionally. In a negligence lawsuit, the plaintiff is the party bringing the claim, while the defendant is the party accused of causing harm. To prevail in a negligence claim, the plaintiff must establish the following elements:

- Duty of Care: The defendant had a legal obligation to adhere to a specific standard of conduct to protect others, including the plaintiff, from unreasonable risks.
- Breach of Duty: The defendant failed to meet the required standard of care.[9]
- Causation: The defendant's breach caused the plaintiff's injury.

---

[2] Art. I, s. 21, FLA. CONST.

[3] *Kluger v. White*, 281 So. 2d 1 (Fla. 1973).

[4] *See Achord v. Osceola Farms Co.,* 52 So. 3d 699 (Fla. 2010).

[5] *See Anderson v. Gannett Comp.*, 994 So. 2d 1048 (Fla. 2008) (false light was not actionable under the common law); *McPhail v. Jenkins*, 382 So. 2d 1329 (Fla. 1980) (wrongful death was not actionable under the common law); *see also Kluger*, 281 So. 2d at 4 ("We hold, therefore, that where a right of access to the courts for redress for a particular injury has been provided by statutory law predating the adoption of the Declaration of Rights of the Constitution of the State of Florida, or where such right has become a part of the common law of the State . . . the Legislature is without power to abolish such a right without providing a reasonable alternative . . . unless the Legislature can show an overpowering public necessity . . . .").

[6] *Kluger*, 281 So. 2d at 4; *see Univ. of Miami v. Echarte*, 618 So. 2d 189 (Fla. 1993) (upholding a statutory cap on medical malpractice damages because the Legislature provided arbitration, which is a "commensurate benefit" for a claimant); *accord Lasky v. State Farm Ins. Co*., 296 So. 2d 9 (Fla. 1974); *Smith v. Dept. of Ins*., 507 So. 2d 1080 (Fla. 1992) (striking down a noneconomic cap on damages, which, while not wholly abolishing a cause of action, did not provide a commensurate benefit).

[7] *Kluger*, 281 So. 2d at 4-5 (noting that in 1945, the Legislature abolished the right to sue for several causes of action, but successfully demonstrated "the public necessity required for the total abolition of a right to sue."); *see Echarte*, 618 So. 2d at 195 ("Even if the medical malpractice arbitration statutes at issue did not provide a commensurate benefit, we would find that the statutes satisfy the second prong of Kluger which requires a legislative finding that an 'overpowering public necessity' exists, and further that 'no alternative method of meeting such public necessity can be shown.'").

[8] *See* 74 Am. Jur. 2d Torts § 2.

[9] However, in a negligence per se case, the plaintiff does not need to prove breach of duty, as it is established as a matter of law. Black's Law Dictionary (12th ed.), negligence.

- Damages: The plaintiff suffered actual harm, such as physical injury, financial loss, or other measurable damages.[10]

Courts recognize different levels of negligence, which can impact liability and potential damages:
- Slight Negligence: A minor failure to exercise great care, often applied to common carriers (e.g., public transportation providers) that have a heightened duty to ensure passenger safety.[11]
- Ordinary Negligence: The failure to exercise reasonable care that a prudent person would use under similar circumstances, resulting in foreseeable harm.[12]
- Gross Negligence: A reckless disregard for the safety of others, demonstrating a conscious indifference to known risks. Unlike ordinary negligence, gross negligence often requires proof that the defendant was aware of imminent danger yet failed to act. A finding of gross negligence may justify an award of punitive damages,[13] which are meant to punish and deter particularly egregious conduct.[14]

Comparative Negligence and Pleading Standards in Florida
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.[15] 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.

Florida follows the fact-pleading standard, which requires plaintiffs in civil cases to file a complaint that includes:
- A short and plain statement of the court's jurisdiction, unless jurisdiction is already established.
- A concise statement of the ultimate facts[16] supporting the claim.
- A demand for relief, specifying what the plaintiff seeks (e.g., monetary damages, injunctions, etc.).[17]

Certain claims must be pleaded with particularity, meaning the complaint must include detailed factual allegations sufficient to establish each element of the claim. This heightened standard applies to allegations such as fraud, mistake, or conditions of the mind, requiring more than general assertions.[18]

Burden of Proof and Legal Presumptions
The *burden of proof* refers to the obligation to establish a material fact in a legal dispute.[19] Generally, the party asserting a fact bears the burden.[20] 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

---

[10] *See* 21 Fla. Prac., Elements of an Action § 1401:1 (2024-2025 ed.); *see also Barnett v. Dept. of Financial Services*, 303 So.3d 508 (Fla. 2020).
[11] Black's Law Dictionary (12th ed. 2024), negligence; *see also Faircloth v. Hill*, 85 So. 2d 870 (Fla. 1956); *Holland America Cruises, Inc. v. Underwood*, 470 So. 2d 19 (Fla. 2d DCA 1985); *Werndli v. Greyhound Corp*., 365 So. 2d 177 (Fla. 2d DCA 1978).
[12] Black's Law Dictionary (12th ed. 2024), negligence; *see also De Wald v. Quarnstrom*, 60 So. 2d 919 (Fla. 1952); *Clements v. Deeb* , 88 So. 2d 505 (Fla. 1956).
[13] Punitive damages are awarded in addition to actual damages to punish a defendant for behavior considered especially harmful. Florida generally caps punitive damage awards at $500,000 or triple the value of compensatory damages, whichever is greater, and caps cases of intentional misconduct with a financial motivation at two million dollars or four times the amount of compensatory damages, whichever is greater. However, if the defendant intended to harm the claimant and actually caused harm, punitive damages are not capped. S. 768.73(1), F.S.
[14] Black's Law Dictionary (12th ed. 2024), negligence; s. 768.72(2)(b), F.S.; *see also* Clements, 88 So. 2d 505 (Fla. 1956); *Carraway v. Revell*, 116 So. 2d 16 (Fla. 1959); Glaab v. Caudill, 236 So. 2d 180 (Fla. 2d DCA 1970).
[15] S. 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, to any action based on an intentional tort, or to any action as to which application of the doctrine of joint and several liability is specifically provided by ch. 403, 517, 542, and 895, F.S. *See* s. 768.81(4), F.S.
[16] An ultimate fact is a fact that is essential to the claim or defense. Black's Law Dictionary (12th ed.), fact.
[17] Fla. R. Civ. P. 1.110; s*ee also Goldschmidt v. Holman*, 571 So. 2d 422 (Fla. 1990).
[18] This heightened standard also applies to claims involving denial of performance or occurrence. Fla. R. Civ. P. 1.120(b) and (c).
[19] Black's Law Dictionary (12th ed. 2024), burden of proof.
[20] *See Berg v. Bridle Path Homeowners Ass'n, Inc*., 809 So. 2d 32 (Fla. 4th DCA 2002).

defense—whether in a civil or criminal case—must prove the elements of that defense.[21] In some instances, statutory or common law presumptions shift the burden of proof to the opposing party and generally remain in effect unless sufficiently rebutted.[22]

Sovereign Immunity

Sovereign immunity is a legal doctrine that prevents the government from being sued without its consent.[23] The Florida Constitution allows the Legislature to waive this immunity,[24] and 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.[25] 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.[26]

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[27] granting additional compensation.[28]

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.[29] 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.[30]

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.[31]

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. For a class action to be certified, the court must find that the case meets specific legal requirements, including:

- Numerosity: The class is large enough to justify a class action.
- Commonality: Class members share common legal or factual issues.
- Typicality: The lead plaintiff's claims are representative of the class.
- Adequacy: The lead plaintiff and attorneys can fairly and adequately represent the class.[32]

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 binding on all class members, who are generally prohibited from filing individual lawsuits raising the same claim. Notably, a class may include individuals harmed

---

[21] 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.
[22] *See* Black's Law Dictionary (12th ed. 2024), presumption; Cornell Law School, *Presumption* (last visited March 15, 2025).
[23] Cornell Law School, *Sovereign Immunity* (last visited March 17, 2025).
[24] Art. X, s. 13, FLA. CONST.
[25] S. 768.28(1), F.S.
[26] *Id.*
[27] A "claim bill" is a bill that presents a claim to compensate a particular individual or entity for injuries or losses caused by the negligence or error of a public officer or agency. The Florida Senate, *Glossary* (last visited March 17, 2025).
[28] S. 768.28(5)(a), F.S.
[29] S. 768.28(9)(a), F.S.
[30] *Id.*
[31] Cornell Law School, *Class Action* (last visited March 17, 2025).
[32] *See* Fla. R. of Civ. Procedure 1.220; Fed. R. Civ. P. 23.; *see also Sosa v. Safeway Premium Fin. Co.*, 73 So. 3d 91 (Fla. 2011).

in the same manner as other class members without ever receiving direct notice of the action, making class certification an important judicial safeguard.[33]

Cybersecurity Standards or Frameworks

The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce.[34] 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.[35]

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 and the decision about how to apply it is left to the implementing organization.[36]

In addition to the NIST cybersecurity framework, several other cybersecurity standards, frameworks, and compliance programs apply across industries and use cases:

- *NIST Special Publication 800-171*: Establishes security requirements for protecting controlled unclassified information. Defense contractors and manufacturers in government supply chains must comply with these requirements.[37]
- *NIST Special Publication 800-53 and 800-53A*: Provides a comprehensive catalog of security and privacy controls to help organizations manage cybersecurity risks across various environments, including cloud and on-premises systems. 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.[38]
- *Federal Risk and Authorization Management Program (FedRAMP)*: A security assessment framework for cloud services providers, ensuring compliance with federal cloud security guidelines.[39]
- *Center for Internet Security Critical Security Controls*: A prescriptive, prioritized set of best practices for strengthening cybersecurity posture developed in 2008 to address significant network security issues.[40]
- *International Organization for Standardization/International Electrotechnical Commission 27000-57 Series*: International cybersecurity standards, with ISO 27001 being the most prominent. This standard provides

[33] *See* Cornell Law School, *Class Action* (last visited March 17, 2025).
[34] *See* NIST, *NIST History* (last visited March 16, 2025).
[35] *See* NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* (last visited March 16, 2025).
[36] *See* NIST, *The NIST Cybersecurity Framework (CSF) 2.0* (last visited March 16, 2025).
[37] NIST, *What is the NIST SP 800-171 and Who Needs to Follow It?* (last visited March 17, 2025).
[38] *See* NIST Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (last visited March 17, 2025).
[39] FedRAMP, *Program Basics* (last visited March 17, 2025).
[40] *See* Center for Internet Security, *CIS Critical Security Controls* (last visited March 17, 2025); DOT Security, *Explaining the Critical Security Controls (CSC) by the Center for Internet Security* (last visited March 17, 2025).

a management framework for information security management systems, ensuring the confidentiality, integrity, and availability of sensitive corporate data.[41]
- *HITRUST Common Security Framework*: 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.[42]
- *Service Organization Control Type 2 Framework*: Developed by the American Institute of Certified Public Accountants, this framework ensures that third-party service providers securely store and process client data. Compliance is based on five trust service principles: security, privacy, availability, confidentially, and processing integrity.[43]
- *Secure Controls Framework*: A meta-framework incorporating various cybersecurity and data privacy controls to help organizations build secure and compliant programs.[44]

Industry-Specific Cybersecurity Standards

Certain cybersecurity standards apply when handling specific types of sensitive information:
- Health Insurance Portability and Accountability Act (commonly known as HIPPA) Security Rule:[45] Protects electronic protected health information and requires covered entities to ensure confidentiality, threat detection, and compliance training. Mandatory for healthcare providers, insurers, and business associates handling certain protected information.[46]
- Gramm-Leach-Bliley Act (Title V, 1999):[47] Mandates financial institutions to protect consumer's personal financial data by following privacy regulations set by the Federal Trade Commission.[48]
- Federal Information Security Modernization Act (2014):[49] Requires federal agencies to report the status of their information security programs and undergo annual independent security assessments.[50]
- Health Information Technology for Economic and Clinical Health Act:[51] Strengthens HIPPA enforcement for health data privacy and security, particularly regarding electronic transmissions.[52]
- Criminal Justice Information Services (CJIS) Security Policy: Establishes minimum security standards for criminal justice and non-criminal justice agencies that access the Federal Bureau of Investigation's CJIS Division systems to safeguard sensitive law enforcement data.[53]

Multi-Factor Authentication

Multi-factor authentication (MFA) is a security measure that requires users to verify their identity using at least two factors before accessing an account. These factors fall into three categories: something you know (e.g., passwords or PINs), something you have (e.g., security codes sent to a phone or authentication app), and something you are (e.g., biometrics like fingerprints or facial recognition). MFA significantly reduces the risk of unauthorized access, even if passwords are compromised. According to the industry experts, enabling MFA can prevent 99% of automated hacking attacks.[54]

Local Government Cybersecurity

Current law requires local governments (i.e., counties and municipalities) to implement, adopt, and comply with cybersecurity training, standards, and incident notification protocols.[55] The Florida Digital Service (FLDS) is

---

[41] IT Governance USA Inc., *ISO 27001, the International Information Security Standard* (last visited March 17, 2025).
[42] Linford and Company, LLP, *Understanding the HITRUST CSF: A Guide for Beginners* (last visited March 17, 2025).
[43] OneLogin, *What is SOC 2* (last visited March 17, 2025).
[44] *See* Secure Controls Framework, *SCF Frequently Asked Questions (FAQ)* (last visited March 17, 2025).
[45] 45 C.F.R. §§ 160, 162, 164.
[46] U.S. Department of Health and Human Services, *HIPAA for Professionals* (last visited March 17, 2025).
[47] Pub. L. No. 106-102, as amended.
[48] Federal Trade Commission, *Gramm-Leach-Bliley Act* (last visited March 17, 2025).
[49] Pub. L. No. 113-283.
[50] Chief Information Officers Council, *Federal Information Security Modernization Act (FISMA)* (last visited March 17, 2025).
[51] Pub. L. No. 111-5.
[52] U.S. Department of Health and Human Services, *HITECH Act Enforcement Interim Final Rule* (last visited March 17, 2025).
[53] *See* Federal Bureau of Investigation, *Criminal Justice Information Services (CJIS) Security Policy* (last visited March 17, 2025).
[54] *See* National Cybersecurity Alliance, *What is Multifactor Authentication (MFA) And Why Should You Use It?* (last visited March 17, 2025); *see also* NIST, *Computer Security Resource Center Multi-Factor Authentication (MFA)* (last visited March 17, 2025).
[55] S. 282.3185, F.S.

responsible for developing cybersecurity training for local government employees. All employees with access to a local government's network must complete basic cybersecurity training within 30 days of employment and annually thereafter. Additionally, technology professionals and employees handling highly sensitive information must complete advanced cybersecurity training on the same schedule.[56]

Local governments must also adopt cybersecurity standards that protect their data, information technology (IT), and IT resources while ensuring availability, confidentiality, and integrity. These standards must align with generally accepted best practices, including the NIST Cybersecurity Framework. Once adopted, local governments must notify FLDS as soon as possible.[57]

In the event of a cybersecurity or ransomware incident, local governments must adhere to specific notification protocols. They are required to notify the Cybersecurity Operations Center (COC),[58] the Cybercrime Office of The Department of Law Enforcement (FDLE), and the local sheriff. At a minimum, the notification must include a summary of the incident, the date and location of the most recent data backup—including whether it was affected or stored in the cloud—the types of data compromised, the estimated financial impact, and, in the case of ransomware, the ransom demand details. Additionally, the local government must indicate whether it is requesting assistance from the COC, FDLE, or the sheriff.[59]

Ransomware incidents, as well as cybersecurity incidents classified as severity level 3, 4, or 5, must be reported as soon as possible, but no later than 48 hours after discovery for cybersecurity incidents and 12 hours after discovery for ransomware incidents. The COC must then notify the President of the Senate and Speaker of the House of Representatives within 12 hours of receiving the local government's report, providing a high-level description and the likely effects of the incident. Local governments may also report lower-severity cybersecurity incidents at their discretion. The COC must also submit a consolidated incident report on a quarterly basis to the President of the Senate, Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council (CAC).[60] While the report to the CAC cannot include local government names, network details, or system identifiers, it must contain sufficient information to support the Council's responsibilities.[61]

Following remediation, an after-action report summarizing the incident, resolution, and lessons learned must be submitted to FLDS within one week. This report must include details such as the incident summary, incident resolutions, and any insights gained as a result of the incident.[62]

Florida's Data Breach Notification Laws

Current law requires covered entities,[63] government entities,[64] and third-party agents[65] to take reasonable measures to protect personal information stored in electronic form.[66] If a data breach affects 500 or more

---

[56] S. 282.3185(3), F.S.
[57] S. 282.3185(4), F.S.
[58] The COC, led by the state chief information security officer within FLDS, is a primarily virtual facility staffed with detection and incident response personnel that serves as a clearinghouse for cybersecurity threat information and coordinates with law enforcement. *See* s. 282.318(3)(h), F.S.
[59] S. 282.3185(5)(b), F.S.
[60] The CAC is an advisory body, housed with the Department of Management Services, tasked with assisting state and local government agencies on addressing cybersecurity threats. The CAC provides guidance on best practices, reviews cybersecurity policies, assesses risks, and makes legislative recommendations. It also collaborates with federal agencies and private-sector experts to enhance cybersecurity measures and reports on ransomware trends. *See* s. 282.319, F.S.
[61] S. 282.3185(5)(b), (c), (d), F.S.
[62] S. 282.3185(6), F.S.
[63] "Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. For purposes of the notice requirements, the term includes a governmental entity. S. 501.171(1)(b), F.S.
[64] "Governmental entity" means any department, division, bureau, commission, regional planning agency, board, district, authority, agency, or other instrumentality of this state that acquires, maintains, stores, or uses data in electronic form containing personal information. S. 501.171(1)(f), F.S.
[65] "Third-party agent" means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity. S. 501.171(1)(h), F.S.
[66] S. 501.171(2), F.S.

individuals in the state, covered entities and government entities must notify the Department of Legal Affairs (DLA) as soon as possible but within 30 days of determining that a breach has occurred or is reasonably believed to have occurred. If the entity provides written justification, it may receive an additional 15 days to complete the notification. Notices to the DLA must include a synopsis of the breach, the number of individuals affected, any free services offered, a copy of the individual notification (or explanation of alternative actions taken), and contact information for further inquiries.[67] Upon request, the covered entity must also provide a police report, forensic analysis, breach response policies, and details on remediation efforts.[68]

The entity must also notify affected individuals as soon as possible but no later than 30 days, with reasonable time allowed to assess the breach, identify those affected, and restore system integrity. If a law enforcement agency determines that disclosure would interfere with an active investigation, notification may be delayed for a specified period upon written request. Additionally, if the entity determines—after investigation and consultation with law enforcement—that the breach is unlikely to result in harm, individual notification is not required; however, the entity must document this determination in writing an submit it to the DLA within 30 days.[69]

For breaches impacting more than 1,000 individuals, covered entities and government agencies must also notify major nationwide consumer reporting agencies without unreasonable delay.[70] Third-party agents responsible for maintaining, storing, or processing personal information on behalf of a covered entity or government entity must notify the entity of a breach within 10 days of discovering it.[71]

A violation of these provisions constitutes an unfair or deceptive trade practice. DLA may take legal action to obtain a declaratory judgement, issue injunctions, or seek damages on behalf of affected consumers or government entities.[72] Failure to comply with breach notification requirements may result in civil penalties of up to $500,000. Violators are subject to a $1,000 per day fine for the first 30 days of noncompliance, increasing to $50,000 per additional 30-day period, up to 180 days. If the violation extends beyond 180 days, total penalties cannot exceed $500,000.[73]

RECENT LEGISLATION:

YEAR	BILL #	HOUSE SPONSOR(S)	SENATE SPONSOR	OTHER INFORMATION
2024	CS/CS/HB 473	Giallombardo, Steele	DiCeglie	The bill was vetoed by the Governor.

[67] Judicial branch entities, the Executive Office of the Governor, the Department of Financial Services, and the Department of Agriculture and Consumer Services may fulfill breach notification requirements by posting the required information on an agency-managed website instead of submitting written notification to DLA. S. 501.171(3)(e), F.S.
[68] S. 501.171(3), F.S.
[69] S. 501.171(4), F.S.
[70] S. 501.171(5), F.S.
[71] S. 501.171(6), F.S.
[72] S. 501.171(9)(a), F.S.
[73] S. 501.171(9)(b), F.S.

BILL HISTORY

COMMITTEE REFERENCE	ACTION	DATE	STAFF DIRECTOR/ POLICY CHIEF	ANALYSIS PREPARED BY
Information Technology Budget & Policy Subcommittee	14 Y, 2 N, As CS	3/25/2025	Davila	Villa
THE CHANGES ADOPTED BY THE COMMITTEE:	The amendment: • Defined the terms "disaster recovery" and "personal information." • Expanded the bill's liability protections related to cybersecurity incidents to include all political subdivisions of the state. • Removed application to the Local Government Cybersecurity Grant Program and sharing telemetry data as one of the measures to obtain liability protection. • Replaced a blanket liability shield for covered entities and third-party agents in class actions with a presumption against liability. • Applied the presumption against liability to any putative class action that is not certified as of the bill's effective date.			
Civil Justice & Claims Subcommittee				
State Affairs Committee				

THIS BILL ANALYSIS HAS BEEN UPDATED TO INCORPORATE ALL OF THE CHANGES DESCRIBED ABOVE.
