HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: PCS for CS/HB 473 Cybersecurity Incident Liability
SPONSOR(S): Judiciary Committee
TIED BILLS: **IDEN./SIM. BILLS:**

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
Orig. Comm.: Judiciary Committee		Leshko	Kramer

SUMMARY ANALYSIS

Section 282.3185, F.S., requires counties and municipalities (referred to as local governments in this section) to implement, adopt, and comply with cybersecurity training, standards, and incident notification protocols. Local governments are required to adopt cybersecurity standards that safeguard the local government's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute for Standards and Technology (NIST) Cybersecurity Framework.

NIST is a non-regulatory federal agency housed within the United States Department of Commerce, whose role is to facilitate and support the development of cybersecurity risk frameworks. NIST is charged with providing a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks. While the NIST Cybersecurity Framework was developed with critical infrastructure in mind, it can also be used by organizations in any sector of the economy or society.

Additionally, s. 501.171, F.S., requires covered entities, governmental entities, and third-party agents to comply with specified notification protocols in the event of a breach of security affecting personal information.

PCS for CS/HB 473 creates s. 768.401, F.S., to provide that a county or municipality that substantially complies with the cybersecurity training, standards, and notification protocols under s. 282.3185, F.S., or any other political subdivision of the state that complies with s. 282.3185, F.S., on a voluntary basis, is not liable in connection with a cybersecurity incident.

The bill also provides that a covered entity or third-party agent, that acquires, maintains, stores, processes, or uses personal information is not liable in connection with a cybersecurity incident if the covered entity or third-party agent substantially complies with notice protocols as provided within s. 501.171, F.S., as applicable, and has also adopted a cybersecurity program that substantially aligns with the current version of any standards, guidelines, or regulations that implement any of the standards specified in the bill or with applicable state and federal laws and regulations. The bill provides certain requirements for a covered entity or third-party agent to retain its liability protection.

The bill does not establish a private cause of action. The bill further provides that the amendments made by the bill apply to any suit filed on or after the effective date of the bill and to any putative class action not certified on or before the effective date of the bill.

The bill does not affect state or local government revenues or expenditures.

The bill takes effect upon becoming law.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Present Situation

Access to Courts

The Florida Constitution broadly protects the right to access the courts, which "shall be open to every person for redress of any injury...."[1] However, this constitutional right is not unlimited.

In *Kluger v. White*,[2] the Supreme Court of Florida stated that it would not completely prohibit the Legislature from altering a cause of action, but neither would it allow the Legislature "to destroy a traditional and long-standing cause of action upon mere legislative whim...." The takeaway from *Kluger* and other relevant case law is that the Legislature may:

- Reduce the right to bring a cause of action as long as the right is not entirely abolished.[3]
- Abolish a cause of action that is not "traditional and long-standing"—that is, a cause of action that did not exist at common law, and that did not exist in statute before the adoption of the Florida Constitution's Declaration of Rights.[4]
- Abolish a cause of action if the Legislature either:
    - Provides a reasonable commensurate benefit in exchange;[5] or
    - Shows an "overpowering public necessity for the abolishment of such right, and no alternative method of meeting such public necessity can be shown."[6]

Tort Liability and Negligence

A "tort" is a wrong for which the law provides a remedy. The purpose of tort law is to fairly compensate a person harmed by another person's wrongful acts, whether intentional, reckless, or negligent, through a civil action or other comparable process. A properly-functioning tort system:

- Provides a fair and equitable forum to resolve disputes;
- Appropriately compensates legitimately harmed persons;
- Shifts the loss to responsible parties;
- Provides an incentive to prevent future harm; and
- Deters undesirable behavior.[7]

"Negligence" is a legal term for a type of tort action that is unintentionally committed. In a negligence action, the plaintiff is the party that brings the lawsuit, and the defendant is the party that defends against it. To prevail in a negligence lawsuit, a plaintiff must demonstrate that the:

- Defendant had a legal duty of care requiring the defendant to conform to a certain standard of conduct for the protection of others, including the plaintiff, against unreasonable risks;
- Defendant breached his or her duty of care by failing to conform to the required standard;

---

[1] Art. I, s. 21, Fla. Const.
[2] *Kluger v. White*, 281 So. 2d 1 (Fla. 1973).
[3] *See Achord v. Osceola Farms Co.*, 52 So. 3d 699 (Fla. 2010).
[4] *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. . . .").
[5] *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); *but see 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).
[6] *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") (citing *Rotwein v. Gersten*, 36 So. 2d 419 (Fla. 1948); *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'").
[7] Am. Jur. 2d Torts s. 2.

- Defendant's breach caused the plaintiff's injury; and
- Plaintiff suffered actual damage or loss resulting from his or her injury.[8]

Courts distinguish varying degrees of civil negligence by using terms such as:

Slight Negligence	The failure to exercise great care. This often applies to injuries caused by common carriers charged with the duty to exercise the highest degree of care toward their passengers.[9]
Ordinary Negligence	The failure to exercise that degree of care which an ordinary prudent person would exercise; or, in other words, a course of conduct which a reasonable and prudent person would know might possibly result in injury to others.[10]
Gross Negligence	A course of conduct which a reasonable and prudent person knows would probably and most likely result in injury to another.[11] To prove gross negligence, a plaintiff must usually show that the defendant had knowledge or awareness of imminent danger to another and acted or failed to act with a conscious disregard for the consequences.[12] Once proven, gross negligence may support a punitive damage[13] award.[14]

In Florida, before a court awards damages in a negligence action, the jury generally assigns a fault percentage to each party under the comparative negligence rule. Florida applies[15] a "modified" comparative negligence rule, which generally prohibits a plaintiff from recovering damages if the plaintiff is more than 50 percent at fault for his or her own harm.[16]

The Florida Rules of Civil Procedure generally require a plaintiff in a civil action to file a complaint and require a defendant to file an answer to the complaint.[17] Florida is a "fact-pleading jurisdiction." This means that a pleading setting forth a claim for relief, including a complaint, must generally state a cause of action and contain a:

- Short and plain statement of the grounds on which the court's jurisdiction depends, unless the court already has jurisdiction and the claim needs no new grounds to support it;
- Short and plain statement of the ultimate facts[18] showing the pleader is entitled to relief; and
- Demand for the relief to which the pleader believes he or she is entitled.[19]

---

[8] 6 *Florida Practice Series* s. 1.1; *see Barnett v. Dept. of Financial Services*, 303 So. 3d 508 (Fla. 2020).
[9] *See Faircloth v. Hill*, 85 So. 2d 870 (Fla. 1956); *see also 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); 6 *Florida Practice Series* s. 1.2.
[10] *See De Wald v. Quarnstrom*, 60 So. 2d 919 (Fla. 1952); *see also Clements v. Deeb*, 88 So. 2d 505 (Fla. 1956); 6 *Florida Practice Series* s. 1.2.
[11] *See Clements*, 88 So. 2d 505; 6 *Florida Practice Series* s. 1.2.
[12] *See Carraway v. Revell*, 116 So. 2d 16 (Fla. 1959).
[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. S. 768.73(1), F.S.
[14] *See Glaab v. Caudill*, 236 So. 2d 180 (Fla. 2d DCA 1970); 6 *Florida Practice Series* s. 1.2; s. 768.72(2), F.S.
[15] The comparative negligence standard does not apply to any action brought to recover economic damages from pollution, based on an intentional tort, or to which the joint and several liability doctrines is specifically applied in ch. 403, 498, 517, 542, and 895, F.S. S. 768.81(4), F.S.
[16] 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.; therefore, a plaintiff who is more than fifty percent responsible for his or her own damages may still recover a portion of damages in a medical negligence suit.
[17] Fla. R. Civ. P. 1.100.
[18] Ultimate facts are facts that must be accepted for a claim to prevail, usually inferred from a number of supporting evidentiary facts, which themselves are facts making other facts more probable. *See* Legal Information Institute, *Ultimate Fact*, https://www.law.cornell.edu/wex/ultimate_fact (last visited Jan. 18, 2024); *see also* Legal Information Institute, *Evidentiary Facts*, https://www.law.cornell.edu/wex/evidentiary_fact (last visited Jan. 18, 2024).
[19] *See Goldschmidt v. Holman*, 571 So. 2d 422 (Fla. 1990); Fla. R. Civ. P. 1.110.

However, certain allegations[20] must be plead with "particularity," which is a heightened level of pleading requiring a statement of facts sufficient to satisfy the elements of each claim.

Burden of Proof and Presumptions

The burden of proof is an obligation to prove a material fact in issue.[21] Generally, the party who asserts the material fact in issue has the burden of proof.[22] In a civil proceeding, for example, the burden of proof is on the plaintiff to prove the allegations contained in his or her complaint. Further, a defendant in either a criminal or a civil proceeding has the burden to prove any affirmative defenses[23] he or she may raise in response to the charges or allegations. However, there are certain statutory and common law presumptions[24] that may shift the burden of proof from the party asserting the material fact in issue to the party defending against such fact.[25] These presumptions remain in effect following the introduction of evidence rebutting the presumption, and the factfinder must decide if such evidence is strong enough to overcome the presumption.[26] A presumption is a legal inference that can be made with knowing certain facts. Most presumptions are able to be rebutted, if proven to be false or thrown into sufficient doubt by the evidence.[27]

Local Government Cybersecurity

Section 282.3185, F.S., requires counties and municipalities (referred to as local governments in this section) to implement, adopt, and comply with cybersecurity training, standards, and incident notification protocols.

The Florida Digital Service is tasked with developing basic and advanced[28] cybersecurity training[29] curriculum for local government employees. All local government employees with access to the local government's network must complete basic cybersecurity training within 30 days after commencing employment and annually thereafter.[30] Additionally, all local government technology professionals and employees with access to highly sensitive information must also complete the advanced cybersecurity training within 30 days after commencing employment and annually thereafter.[31]

Additionally, local governments are required to adopt cybersecurity standards that safeguard the local government's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity.[32] The standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute for Standards and Technology (NIST) Cybersecurity

[20] These allegations include fraud, mistake, condition of the mind, and denial of performance or occurrence. Fla. R. Civ. P. 1.120(b),(c).
[21] 5 *Florida Practice Series* s. 16:1.
[22] *Id.*; *see Berg v. Bridle Path Homeowners Ass'n, Inc.*, 809 So. 2d 32 (Fla. 4th DCA 2002).
[23] An affirmative defense is a defense which, if proven, negates criminal or civil liability even if it is proven that the defendant committed the acts alleged. Examples include self-defense, entrapment, insanity, necessity, and *respondeat superior*. Legal Information Institute, *Affirmative Defense*, https://www.law.cornell.edu/wex/affirmative_defense (last visited Jan. 18, 2024).
[24] These presumptions tend to be social policy expressions, such as the presumption that all people are sane or that all children born in wedlock are legitimate. 5 *Florida Practice Series* s. 16:1.
[25] 5 *Florida Practice Series* s. 16:1.
[26] *Id.*
[27] Legal Information Institute, *Presumption*, https://www.law.cornell.edu/wex/presumption (last visited Jan. 18, 2024).
[28] Advanced cybersecurity training must develop, assess, and document competencies by role and skill level. The training curriculum must include training on the identification of each cybersecurity incident severity level contained in s. 282.318(3)(c)9.a., F.S. S. 282.318(3)(g), F.S.
[29] The training may be provided in collaboration with the Cybercrime Office of the Florida Department of Law Enforcement, a private sector entity, or an institution of the Florida State University System. S. 282.3185(3)(b), F.S.
[30] S. 282.3185(3)(a)1., F.S.
[31] S. 282.3185(3)(a)2., F.S.
[32] S.282.3185(4)(a), F.S.

Framework.[33] Once the standards are adopted,[34] each local government is to notify the Florida Digital Service (FLDS)[35] as soon as possible.[36]

Local governments are also required to comply with specified incident notification protocols in the event of a cybersecurity incident or ransomware incident, including:

- Notifying the Cybersecurity Operations Center (COC) of the Cybercrime Office of the Florida Department of Law Enforcement and the sheriff who has jurisdiction over the local government.
    - A local government must report all ransomware incidents and any cybersecurity incident determined by the local government to be of severity level 3, 4, or 5[37] 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.
        - The COC must notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 as soon as possible but no later than 12 hours after receiving the local government's incident report. Such notification must include a high-level description of the incident and the likely effects.
    - A local government may report a cybersecurity incident determined by the local government to be of severity level 1 or 2.[38]
- Submitting an after-action report to the Florida Digital Service within one week after the remediation of a cybersecurity or ransomware incident.
    - The after-action report must summarize the incident, the incident's resolution, and any insights gained as a result of the incident.[39]

Any such local government notification report must contain, 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 incident.
- The estimated fiscal impact of the incident.
- In the case of a ransomware incident, the details of the ransom demanded.[40]

Cybersecurity Standards

NIST is a non-regulatory federal agency housed within the United States Department of Commerce.[41] NIST's role was updated in the Cybersecurity Enhancement Act (CEA) of 2014 to facilitate and support the development of cybersecurity risk frameworks. The CEA charged NIST with providing a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure[42] to help them identify, assess, and manage cyber risks. This charge formalized "NIST's previous work developing Framework Version 1.0 under Executive Order 13636, 'Improving Critical Infrastructure Cybersecurity,' issued in February 2013, and provided guidance for future Framework evolution."[43]

---

[33] *Id*.
[34] Each county with a population of 75,000 or more and each municipality with a population of 25,000 or more were required to adopt such cybersecurity standards by January 1, 2024. However, each county with a population of less than 75,000 and each municipality with a population of less than 25,000 have until January 1, 2025 to adopt appropriate standards. S. 282.3185(4)(b) – (c), F.S.
[35] FLDS works under Department of Management Services to implement policies for information technology and cybersecurity for state agencies.
[36] S.282.3185(4)(d), F.S.
[37] Severity levels are determined based on the criteria contained in s. 282.3185(3)(c)9.a.(I) – (V), F.S.
[38] S. 282.3185(5)(b) – (c), F.S.
[39] S. 282.3185(6), F.S.
[40] S. 282.3185(5)(a), F.S.
[41] NIST, *NIST General Information*, https://www.nist.gov/director/pao/nist-general-information (last visited Feb. 12, 2024).
[42] "Critical infrastructure" is defined as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, p. 1, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited Feb. 11, 2024).
[43] *Id*.

While the Framework was developed with critical infrastructure in mind, it can also be used by organizations in any sector of the economy or society. The Framework is designed to complement, and not replace, an organization's own unique approach to cybersecurity 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. For example, an organization may use its current processes and consider the Framework to identify opportunities to strengthen its cybersecurity risk management. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one. The Framework,[44] overall, provides an outline of best practices that helps organizations decide where to focus resources for cybersecurity protection.[45]

Other cybersecurity standards include:

NIST special publication 800-171	Provides recommended requirements for protecting the confidentiality of controlled unclassified information. Defense contractors must implement the recommended requirements to demonstrate their provision of adequate security to protect the covered defense information included in their defense contracts. Additionally, if a manufacturer, involved in supply chains tied to government contracts, 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.[46]
NIST special publications 800-53 and 800-53A	Contains a catalog of security and privacy controls designed to help protect organizations, assets, the privacy of individuals and to manage cybersecurity and privacy risks in cloud computing environments.[47]
The Federal Risk and Authorization Management Program (FedRAMP) security assessment framework	Provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services and cloud products offered by cloud service providers (CSPs). The FedRAMP authorization process determines whether CSPs meet federal cloud security guidelines. At the core of FedRAMP is the NIST Special Publication 800-53.[48, 49]
The Center for Internet Security (CIS) Critical Security Controls	CIS Critical Security Controls are a prescriptive, prioritized, 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.[50]

[44] NIST Cybersecurity Framework 2.0 is to be released at the end of February 2024.
[45] *Id.* at p. 3.
[46] 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 Feb. 11, 2024).
[47] 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. 11, 2024).
[48] RiskOptics, *How State and Local Agencies Can Use FedRAMP*, https://reciprocity.com/how-state-and-local-agencies-can-use-fedramp/ (last visited Feb. 11, 2024).
[49] Although state and local agencies are not authorized to directly access FedRAMP security documentation (which is housed in a secured federal portal), they can still apply the FedRAMP framework in their own cloud contracts and assessments. *Id*.
[50] CIS, *CIS Critical Security Controls*, https://www.cisecurity.org/controls (last visited Feb. 11, 2024).

The International Organization for Standardization/International Electrotechnical Commission 27000 – series (ISO/IEC 27000) family of standards	The mainstay of the ISO/IEC 27000 family series is ISO 27001, which sets out the specification for an information security management system (ISMS).[51] ISO 27001 is an international standard that helps organizations manage the security of their information assets. ISO 27001 provides a management framework for implementing an ISMS to ensure the confidentiality, integrity, and availability of all corporate data such as, financial information, intellectual property, employee data, and information managed by third parties. ISO 27001 audits can be conducted to review an organization's practices, policies, and procedures to determine if the organization's ISMS meets the requirements of the standard.[52]
HITRUST Common Security Framework (CSF)	The CSF can be utilized to manage and certify compliance with information security controls and to consolidate compliance reporting requirements. The CSF normalizes security and privacy requirements for organizations from a variety of sources, including: HIPPA security requirements; NIST 800-53, and other industry frameworks. The CSF helps organizations consolidate these various sources into a single control set.[53]
Service Organization Control Type 2 (SOC 2) Framework	SOC 2 is a cybersecurity compliance framework developed by the American Institute of Certified Public Accountants. The primary purpose of SOC 2 is to ensure that third-party service providers store and process client data in a secure manner. The framework specifies criteria to uphold high standards of data security, based on five trust service principles: security, privacy, availability, confidentiality, and processing integrity. SOC 2 is able to provide different requirements for every organization depending on the organizations operating models.[54]
Secure Controls Framework	Secure Controls Framework is a metaframework that contains a variety of cybersecurity and data privacy controls that organizations can use to build secure and compliant cybersecurity and data privacy programs.[55]

Additionally, there are certain cybersecurity standards that apply when certain information is being maintained:

[51] IT Governance, *ISO 27000 Series of Standards*, https://www.itgovernanceusa.com/iso27000-family (last visited Feb. 11, 2024).
[52] IT Governance, *ISO 27001, the International Information 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 Feb. 11, 2024).
[53] Linford & Co., LLP, *Understanding the HITRUST CSF: A Guide for Beginners*, https://linfordco.com/blog/hitrust-csf-framework/ (last visited Feb. 16, 2024) (The CSF is updated roughly annually with minor versions being released between major revisions).
[54] One Login, *What is SOC 2?* https://www.onelogin.com/learn/what-is-soc-2#:~:text=SOC%202%2C%20aka%20Service%20Organization%20Control%20Type%202%2C,and%20process%20client%20data%20in%20a%20secure%20manner. (last visited Feb. 16, 2024).
[55] Secure Controls Framework, *About the SCF*, https://securecontrolsframework.com/about-us/ (last visited Feb. 16, 2024); Secure Controls Framework, *SCF Frequently Asked Questions (FAQ)*, https://securecontrolsframework.com/faq/ (last visited Feb. 16, 2024).

The Health Insurance Portability and Accountability Act of 1996 security requirements[56]	The HIPPA Security Rule protects all individually identifiable health information that is created, received, maintained, or transmitted in electronic form. To comply with the HIPAA Security Rule, specified entities must: (1) ensure confidentiality of all electronic protected health information, (2) detect and safeguard against anticipated threats to information security, (3) protect against anticipated impermissible uses or disclosures, and (4) certify compliance by their workforce.[57]
Title V of the Gramm-Leach-Bliley Act of 1999[58]	Requires the Federal Trade Commission, in conjunction with other regulators, to issue regulations ensuring that financial institutions protect the privacy of consumers' personal financial information.[59]
The Federal Information Security Modernization Act of 2014[60]	Requires agencies to report the status of their information security programs to the Office of Management and Budget and requires Inspectors General to conduct annual independent assessments of those programs.[61]
The Health Information Technology for Economic and Clinical Health Act requirements[62]	Addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.[63]
The Criminal Justice Information Services (CJIS) Security Policy	CJIS provides criminal justice agencies and non-criminal justice agencies with a minimum set of security requirements for access to Federal Bureau of Investigation CJIS Division systems and information and to protect and safeguard criminal justice information.[64]

Security of Confidential Personal Information

Section 501.171, F.S., requires covered entities,[65] governmental entities,[66] and third-party agents[67] to take reasonable measures to protect and secure data in electronic form containing personal information.[68, 69]

[56] In 45 C.F.R. part 160 and part 164 subparts A and C.
[57] Centers for Disease Control and Prevention, *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, https://www.cdc.gov/phlp/publications/topic/hipaa.html (last visited Feb. 11, 2024).
[58] Pub. L. No. 106-102, as amended.
[59] Federal Trade Commission, *Gramm-Leach-Bliley Act*, https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act (last visited Feb. 11, 2024).
[60] Pub. L. No. 113-283.
[61] U.S. Chief Information Officers Council, *Federal Information Security Modernization Act (FISMA)*, https://www.cio.gov/policies-and-priorities/FISMA/ (last visited Feb. 11, 2024).
[62] 45 C.F.R. parts 160 and 164.
[63] U.S. Department of Health and Human Services, *HITECH Act Enforcement Interim Final Rule*, https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html (last visited Feb. 11, 2024).
[64] Federal Bureau of Investigation, *Criminal Justice Information Services (CJIS) Security Policy*, https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view (last visited Feb. 16, 2024).
[65] "Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. S. 501.171(1)(b), F.S.
[66] "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.
[67] "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.
[68] S. 501.171(2), F.S.
[69] "Personal information" means either of the following:

Covered entities and governmental entities are required to provide notice to the Department of Legal Affairs (DLA) of any breach of security affecting 500 or more individuals in this state. Such notice must be provided as expeditiously as practicable, but no later than 30 days after the determination of a breach or reason to believe a breach occurred.[70] Additionally, such entities must give notice to each individual in this state whose personal information was, or such entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals must be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred.[71, 72]

Additionally, if a covered entity or governmental entity discovers circumstances that require notice to more than 1,000 individuals at a single time, the entity must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis[73] of the timing, distribution, and content of the notices sent to such individuals.[74]

Third-party agents are required to notify the covered entity or governmental entity, whose personal information it is maintaining, storing, or processing, of a breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred.[75]

A violation of s. 501.171, F.S., is treated as an unfair or deceptive trade practice in any action brought by DLA under s. 501.207, F.S., against a covered entity or third-party agent.

Section 501.207, F.S., authorizes DLA to bring an action:

- To obtain a declaratory judgment that an act or practice violates the Florida Deceptive and Unfair Trade Practices Act (FDUTPA).[76]
- To enjoin any person who has violated, is violating, or is otherwise likely to violate, FDUTPA.
- On behalf of one or more consumers or governmental entities for the actual damages caused by an act or practice in violation of FDUTPA.[77]

---

a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(I) A social security number;

(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(III) 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;

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable. S. 501.171(1)(g), F.S.

[70] S. 501.171(3)(a), F.S.

[71] S. 501.171(4)(a), F.S.

[72] Notice is not required if the entity reasonably determines that 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. S. 501.171(4)(c), F.S.

[73] As defined in the Fair Credit Reporting At, 15 U.S.C. § 1681a(p).

[74] S. 501.171(5), F.S.

[75] S. 501.171(6), F.S.

[76] FDUTPA is a consumer and business protection measure that prohibits unfair methods of competition, unconscionable, deceptive, or unfair acts or practices in the conduct of trade or commerce. FDUTPA was modeled after the Federal Trade Commission Act. S. 501.202, F.S.

[77] S. 501.207(1), F.S.

In additional to the above-enumerated remedies, a covered entity that violates notice requirements to DLA and individuals as provided under s. 501.171, F.S., is liable for a civil penalty[78] not to exceed $500,000, as follows:

- In the amount of $1,000 for each day up to the first 30 days following any notification violation and, thereafter, $50,000 for each subsequent 30-day period or portion thereof for up to 180 days.
- If the violation continues for more than 180 days, in an amount not to exceed $500,000.[79]

Effect of the Bill

PCS for CS/HB 473 creates s. 768.401, F.S., to provide that a county or municipality that substantially complies with the cybersecurity training, standards, and notification protocols under s. 282.3185, F.S., or any other political subdivision of the state that complies with s. 282.3185, F.S., on a voluntary basis, is not liable in connection with a cybersecurity incident.

The bill defines the following terms:

- "Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity.
- "Third-party agent" means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity.

The bill provides that a covered entity or third-party agent that acquires, maintains, stores, processes, or uses personal information is not liable in connection with a cybersecurity incident if the entity or third-party agent substantially complies with the notice protocols required under s. 501.171, F.S., and either:

- Has adopted a cybersecurity program that substantially aligns with the current version of any standards, guidelines, or regulations that implement any of the following:
    - NIST Framework for Improving Critical Infrastructure Cybersecurity;
    - NIST special publication 800-171;
    - NIST special publications 800-53 and 800-53A;
    - The Federal Risk and Authorization Management Program security assessment framework;
    - CIS Critical Security Controls;
    - The International Organization for Standardization/International Electrotechnical Commission 27000 – series family of standards;
    - HITRUST Common Security Framework (CSF);
    - Service Organization Control Type 2 (SOC 2) Framework;
    - Secure Controls Framework;
    - Other similar industry frameworks or standards; or
- If regulated by the state or federal government, or both, or if otherwise subject to the requirements of any of the following laws and regulations, has substantially aligned its cybersecurity program to the current version of:
    - The security requirements of the Health Insurance Portability and Accountability Act of 1996;
    - Title V of the Gramm-Leach-Bliley Act of 1999, as amended;
    - The Federal Information Security Modernization Act of 2014;
    - The Health Information Technology for Economic and Clinical Health Act;
    - The Criminal Justice Information Services (CJIS) Security Policy; or
    - Other similar requirements mandated by state or federal law or regulation.

The bill provides that a covered entity or third-party agent may demonstrate "substantial alignment" with the relevant frameworks, standards, laws, or regulations by providing documentation or other evidence reflecting such alignment following an assessment conducted internally or by a third party. In determining whether a covered entity's or third-party agent's cybersecurity program is in substantial alignment, all of the following factors must be considered:

[78] The civil penalties for failure to notify apply per breach and not per individual affected by the breach. S. 501.171(9)(b), F.S.
[79] S. 501.171(9)(b)1.-2., F.S.

- The size and complexity of the covered entity or third-part agent;
- The nature and scope of the activities of the covered entity or third-party agent; and
- The sensitivity of the information to be protected.

The bill requires a covered entity or third-party agent to make changes as necessary to substantially align its cybersecurity program with any revisions of relevant frameworks or standards or of applicable laws or regulations within one year after the implementation of such revisions, in order to retain protection from liability.

In an action in connection with a cybersecurity incident, if the defendant is a county, municipality, other political subdivision, covered entity, or third-party agent covered by s. 768.401, F.S., the defendant has the burden of proof to establish substantial compliance.

The bill does not establish a private cause of action. It provides that the failure of a county, municipality, other political subdivision of the state, covered entity, or third-party agent to substantially implement a cybersecurity program as specified in the bill is not evidence of negligence and does not constitute negligence per se.

The bill further provides that the amendments made by the bill apply to any suit filed on or after the effective date of the bill and to any putative class action[80] not certified on or before the effective date of the bill.

The bill provides that the act shall take effect upon becoming law.

B. SECTION DIRECTORY:

Section 1: Creates s. 768.401, F.S., relating to limitation on liability for cybersecurity incidents.

Section 2: Provides that the bill is effective upon becoming law.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   None.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

[80] "A putative class action is a lawsuit brought by one or more named plaintiffs on behalf of a potential group of similarly situated individuals (known as a class) who allegedly suffered a common claim. Lawsuits do not become class actions until an actual class has been certified by the court. Therefore, a putative class action means the class has not yet been certified by the court. If the court certifies the class, the lawsuit becomes a class action." International Risk Management Institute, *Putative Class Action*, https://www.irmi.com/term/insurance-definitions/putative-class-action#:~:text=A%20putative%20class%20action%20is,allegedly%20suffered%20a%20common%20claim (last visited Feb. 12, 2024).

The bill may have an indeterminate positive fiscal impact on private individuals as it provides an incentive for counties, municipalities, other political subdivisions, covered entities, and third-party agents to take actions that better protect data (including taxpayer and consumer personal information), information technology, and information technology resources that, if accessed by unauthorized persons, could cause harm to persons and businesses. This action may reduce the frequency and impact of cyber-attacks on private individuals in the state.

The bill may also make it more difficult for plaintiffs to recover damages in a cybersecurity action against entities that comply with the standards outlined in the bill.

D. FISCAL COMMENTS:

The bill does not affect state or local government revenues or expenditures.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable. This bill does not appear to require counties or municipalities to spend funds or take action requiring the expenditures of funds; reduce the authority that counties or municipalities have to raise revenues in the aggregate; or reduce the percentage of state tax shared with counties or municipalities.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

The bill does not require or authorize rulemaking.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE CHANGES