HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/HB 473 Cybersecurity Incident Liability
SPONSOR(S): Commerce Committee, Giallombardo
TIED BILLS: **IDEN./SIM. BILLS:** SB 658

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Commerce Committee	18 Y, 0 N, As CS	Bauldree	Hamon
2) State Administration & Technology Appropriations Subcommittee	9 Y, 4 N	Mullins	Topp
3) Judiciary Committee			

SUMMARY ANALYSIS

Per Florida law, 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.

The NIST is a non-regulatory federal agency housed within the U.S. Department of Commerce. NIST is charged with providing a prioritized, flexible, repeatable, performance-based, and cost-effective framework that helps owners and operators of critical infrastructure identify, assess, and manage cyber risk. While the framework was developed with critical infrastructure in mind, it can be used by organizations in any sector of the economy or society.

Under the bill, a county or municipality that substantially complies with cybersecurity standards required by Florida law or any other political subdivision of the state that complies on a voluntary basis is not liable in connection with a cybersecurity incident.

The bill also provides that a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity or third-party agent, that acquires, maintains, stores, or uses personal information is not liable in connection with a cybersecurity incident if the entity substantially complies with measures to protect and secure electronic data containing personal information as required by Florida law and has adopted a cybersecurity program that substantially aligns with the current version of any of the standards specified in the bill. The bill provides that the scale and scope of "substantial alignment" with a standard specified in the bill must be based on the size and complexity of the entity or third-party agent, the nature and scope of the activities of the entity or third-party agent, and the sensitivity of the information to be protected.

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, or commercial entity or third-party 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 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:

---

[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 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;
- 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 carries 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 "pure" comparative negligence rule, which allows a plaintiff to recover damages proportional to his or her fault percentage.[16] For example, if a plaintiff is 40 percent at fault for an accident causing the plaintiff's injury and the defendant is 60 percent at fault, the plaintiff would recover 60 percent of his or her damages.

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(2), F.S.; *see Williams v. Davis*, 974 So. 2d 1052 (Fla. 2007).
[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]

Cybersecurity Standards

Per Florida law, 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.[28] The standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute for Standards and Technology (NIST) cybersecurity framework.[29] Once the standards are adopted, each local government is to notify the Florida Digital Service (FLDS)[30] as soon as possible.[31]

NIST is a non-regulatory federal agency housed within the U.S. Department of Commerce. NIST is charged with providing a prioritized, flexible, repeatable, performance-based, and cost-effective framework that helps owners and operators of critical infrastructure identify, assess, and manage cyber risk. While the framework was developed with critical infrastructure in mind, it can be used by organizations in any sector of the economy or society.[32] 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. The framework, overall, provides an outline of best practices that helps organizations decide where to focus resources for cybersecurity protection.[33] Other cybersecurity standards include:

[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] S.282.3185(4)(a), F.S.
[29] *Id*.
[30] FLDS works under Department of Management Services to implement policies for information technology and cybersecurity for state agencies.
[31] S.282.3185(4)(d), F.S.
[32] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited March 7, 2023).
[33] *Id.*

NIST special publication 800-171	Provides recommended requirements for protecting the confidentiality of controlled unclassified information. If a manufacturer is part of a Department of Defense, General Services Administration, NASA, or other state or federal agency supply chain then they must comply with these security requirements.[34]
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.[35]
The Federal Risk and Authorization Management Program security assessment framework	Organization established by the General Services Administration (a federal government program) that provides U.S. federal agencies, state agencies, and their vendors with a standardized set of best practices to assess, adopt, and monitor the use of cloud-based technology services under the Federal Information Security Management Act (FISMA).[36]
CIS Critical Security Controls	The Center for Internet Security (CIS) Critical Security Controls are a prescriptive and simplified set of best practices for strengthening cybersecurity for different organizations. CIS was created in response to extreme data losses experienced by organizations in the U.S. defense industrial base.[37]
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.[38]

Florida law also requires certain covered entities,[39] governmental entities,[40] or third-party agents to take reasonable measures to protect and secure data in electronic form containing personal information.[41]

Effect of the Bill

The bill provides that specified entities that substantially comply with certain standards are not liable in connection with a cybersecurity incident.

[34] 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. 18, 2024).

[35] NIST, *Selecting Security and Privacy Controls: Choosing the Right Approach*, https://www.nist.gov/blogs/cybersecurity-insights/selecting-security-and-privacy-controls-choosing-right-approach (last visited Jan. 18, 2024).

[36] RiskOptics, *How State and Local Agencies Can Use FedRAMP*, https://reciprocity.com/how-state-and-local-agencies-can-use-fedramp/#:~:text=The%20Federal%20Risk%20and%20Authorization%20Management%20Program%20%28FedRAMP%29,cloud%20products%20offered%20by%20cloud%20service%20providers%20%28CSPs%29 (last visited Jan. 18, 2024).

[37] CIS Security, *CIS Critical Security Controls*, https://www.cisecurity.org/controls (last visited Jan. 18, 2024).

[38] 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. 18, 2024).

[39] "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 in subsections (3)-(6), the term includes a governmental entity. S. 501.171(1), F.S.

[40] "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. *Id.*

[41] S. 501.171. F.S.

Under the bill, a county or municipality that substantially complies with cybersecurity standards required by Florida law or any other political subdivision of the state that complies on a voluntary basis is not liable in connection with a cybersecurity incident.

The bill also provides that a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity or third-party agent that acquires, maintains, stores, or uses personal information is not liable in connection with a cybersecurity incident if the entity substantially complies with measures to protect data containing personal information, as required by Florida law, and has adopted a cybersecurity program that substantially aligns with the current version of any of the following:

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

Under the bill, if the entity or third-party agent is regulated by the state or federal government, or both, or is otherwise subject to the requirements of any of the following laws and regulations, it must substantially align its cybersecurity program to the current version of:

- The security requirements of the Health Insurance Portability and Accountability Act of 1996;[42]
- Title V of the Gramm-Leach-Bliley Act of 1999 as amended;[43]
- The Federal Information Security Modernization Act of 2014;[44] or
- The Health Information Technology for Economic and Clinical Health Act.[45]

The bill provides that the scale and scope of the entity's or third-party agent's "substantial alignment" with a standard specified in the bill must be based on the following factors:

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

Under the bill, any commercial entity or third-party agent that substantially complies with a combination of industry-recognized cybersecurity frameworks or standards, including the payment card industry data security standard, gains a presumption against liability in connection with a cybersecurity incident. To maintain this presumption, it must adopt revised frameworks or standards within one year after the latest publication date stated in the revisions. In an action in connection with a cybersecurity incident, if

[42] To comply with the HIPAA Security Rule, covered 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 disclosures, and (4) certify compliance by their workforce. 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 Jan. 19, 2024).

[43] Title V of this Act 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. Federal Trade Commission, *Gramm-Leach-Bliley Act*, https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act (last visited Jan. 19, 2024).

[44] The Federal Information Security Modernization Act requires agencies to report the status of their information security programs to OMB and requires Inspectors General (IG) to conduct annual independent assessments of those programs. U.S. Chief Information Officers Council, *Federal Information Security Modernization Act (FISMA)*, https://www.cio.gov/policies-and-priorities/FISMA/ (last visited Jan. 19, 2024).

[45] The Health Information Technology for Economic and Clinical Health Act 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. 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 Jan. 19, 2024).

the defendant is an entity covered by the bill, the defendant holds 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, or commercial entity or third-party 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 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:

The bill provides an incentive for local governments and certain commercial 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 may reduce the frequency and impact of cyber-attacks in the state.

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

On January 23, 2024, the Commerce Committee adopted two amendments and reported the bill favorably as a committee substitute. The amendments provided that:

- In addition to a county or municipality, a political subdivision of the state that substantially complies with specified cybersecurity standards in Florida law on a voluntary basis is not liable in connection with a cybersecurity incident.
- The failure of a political subdivision of the state to substantially implement a cybersecurity program that is in compliance with the provisions of the bill is not evidence of negligence and does not constitute negligence per se.

This analysis is drafted to the committee substitute as passed by the Commerce Committee.