LEGISLATIVE ACTION

Senate		House
Comm: RCS	.	
02/06/2024	.	
	.	
	.	
	.	
	.	

The Committee on Governmental Oversight and Accountability (DiCeglie) recommended the following:

Senate Amendment (with title amendment)

Delete everything after the enacting clause and insert:

Section 1. Section 768.401, Florida Statutes, is created to read:

768.401 Limitation on liability for cybersecurity incidents.—

(1) A county or municipality that substantially complies with s. 282.3185, and any other political subdivision of the

state that substantially complies with s. 282.3185 on a voluntary basis, is not liable in connection with a cybersecurity incident.

(2) 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 s. 501.171, if applicable, and has:

(a) Adopted a cybersecurity program that substantially aligns with the current version of any standards, guidelines, or regulations that implement any of the following:

1. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

2. NIST special publication 800-171.

3. NIST special publications 800-53 and 800-53A.

4. The Federal Risk and Authorization Management Program security assessment framework.

5. The Center for Internet Security (CIS) Critical Security Controls.

6. The International Organization for Standardization/International Electrotechnical Commission 27000-series (ISO/IEC 27000) family of standards; or

(b) 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, substantially aligned its cybersecurity program to the current version of the following, as applicable:

1. The Health Insurance Portability and Accountability Act of 1996 security requirements in 45 C.F.R. part 160 and part 164 subparts A and C.

2. Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended.

3. The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283.

4. The Health Information Technology for Economic and Clinical Health Act requirements in 45 C.F.R. parts 160 and 164.

(3) The scale and scope of substantial alignment with a standard, law, or regulation under paragraph (2)(a) or paragraph (2)(b) by a covered entity or third-party agent, as applicable, is appropriate if it is based on all of the following factors:

(a) The size and complexity of the covered entity or third-party agent.

(b) The nature and scope of the activities of the covered entity or third-party agent.

(c) The sensitivity of the information to be protected.

(4) Any commercial entity or third-party agent covered by subsection (2) that substantially complies with a combination of industry-recognized cybersecurity frameworks or standards to gain the presumption against liability pursuant to subsection (2) must, upon the revision of two or more of the frameworks or standards with which the entity complies, adopt the revised frameworks or standards within 1 year after the latest publication date stated in the revisions and, if applicable, comply with the Payment Card Industry Data Security Standard (PCI DSS).

(5) This section does not establish a private cause of

action. Failure of a county, municipality, other political subdivision of the state, or commercial entity to substantially implement a cybersecurity program that is in compliance with this section is not evidence of negligence and does not constitute negligence per se.

(6) In an action in connection with a cybersecurity incident, if the defendant is an entity covered by subsection (1) or subsection (2), the defendant has the burden of proof to establish substantial compliance.

Section 2. This act shall take effect upon becoming a law.

================= TITLE AMENDMENT ================

And the title is amended as follows:

Delete everything before the enacting clause

and insert:

A bill to be entitled

An act relating to cybersecurity incident liability; creating s. 768.401, F.S.; providing that a county, municipality, other political subdivision of the state, commercial entity, or third-party agent that complies with certain requirements is not liable in connection with a cybersecurity incident; requiring certain entities to adopt certain revised frameworks or standards within a specified time period; providing that a private cause of action is not established; providing that certain failures are not evidence of negligence and do not constitute negligence per se; specifying that the defendant in certain actions has a certain burden of proof; providing an effective date.