By Senator DiCeglie

A bill to be entitled

An act relating to cybersecurity incident liability; creating s. 768.401, F.S.; defining terms; providing that a county, municipality, other political subdivision of the state, covered entity, or third-party agent that complies with certain requirements is not liable in connection with a cybersecurity incident under certain circumstances; requiring covered entities and third-party agents to align their cybersecurity programs with any revised frameworks, standards, laws, or regulations within a specified time period; providing that a private cause of action is not established; providing that certain failures are not evidence of negligence, do not constitute negligence per se, and cannot be used as evidence of fault; specifying that the defendant in certain actions has a certain burden of proof; providing applicability; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

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

768.401 Limitation on liability for cybersecurity incidents.—

(1) As used in this section, the term:

(a) “Covered entity” means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity.

(b) “Cybersecurity standards or frameworks” means one or more 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 27000-57 series (ISO/IEC 27000) family of standards;

7. HITRUST Common Security Framework (CSF);

8. Service Organization Control Type 2 Framework (SOC 2);

9. Secure Controls Framework; or

10. Other similar industry frameworks or standards, or a reasonable combination of one or more of the above.

(c) “Third-party agent” means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity.

(2) A county or municipality is not liable in connection with a cybersecurity incident if the county or municipality has:

(a)1. One or more policies that substantially align with cybersecurity standards or frameworks;

2. Disaster recovery plans for cybersecurity incidents; and

3. Multi-factor authentication as required by the cybersecurity standards or frameworks relied on in sub-

subparagraph (3)(b)1.a.; or

(b) Applied to the Local Government Cybersecurity Grant Program and shares telemetry data with the state's cybersecurity operations center.

(3) A covered entity or third-party agent that acquires, maintains, stores, processes, or uses personal information is not liable in a class action resulting from a cybersecurity incident if the covered entity or third-party agent does all of the following, as applicable:

(a) Substantially complies with s. 501.171(3)-(6), as applicable.

(b) Has adopted or implemented:

1.a. One or more policies that substantially align with cybersecurity standards or frameworks;

b. A disaster recovery plan for cybersecurity incidents; and

c. Multi-factor authentication as required by the cybersecurity standards or frameworks relied on in sub-subparagraph a.; or

2. 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, a cybersecurity program that substantially aligns with the current version of the following, as applicable:

a. 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.

b. Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended, and its implementing regulations.

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

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

e. The Criminal Justice Information Services (CJIS) Security Policy.

f. Other similar requirements mandated by state or federal law or regulation.

(4) A covered entity’s or third-party agent’s substantial alignment with a framework or standard under subparagraph (3)(b)1. or with a law or regulation under subparagraph (3)(b)2. may be demonstrated by providing documentation or other evidence of an assessment, conducted internally or by a third-party, reflecting that the covered entity’s or third-party agent’s cybersecurity program is substantially aligned with the relevant framework or standard or with the applicable state or federal law or regulation.

(5) Any covered entity or third-party agent must substantially align its cybersecurity program with any revisions of relevant frameworks or standards or of applicable state or federal laws or regulations within 1 year after the latest publication date stated in any such revisions in order to retain protection from liability.

(6) This section does not establish a private cause of action.

(7) Failure of a county, municipality, other political subdivision of the state, covered entity, or third-party agent to substantially implement a cybersecurity program that is in compliance with this section is not evidence of negligence, does

not constitute negligence per se, and cannot be used as evidence of fault under any other theory of liability.

(8) In an action relating to a cybersecurity incident, if the defendant is a county, municipality, or political subdivision covered by subsection (2) or a covered entity or third-party agent covered by subsection (3), the defendant has the burden of proof to establish substantial compliance.

Section 2. The amendments made by this act apply to any putative class action filed on or after the effective date of this act.

Section 3. This act shall take effect upon becoming a law.