A bill to be entitled

An act relating to cybersecurity incident liability; creating s. 768.401, F.S.; providing definitions; 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; requiring covered entities and third-party agents to adopt 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 and do not constitute negligence per se; 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) "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 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.

(3) 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 does all of the following, as applicable:

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

(b)1. Has adopted a cybersecurity program that substantially aligns with the current version of any standards, guidelines, or regulations that implement any of the following:

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

b. NIST special publication 800-171;

c. NIST special publications 800-53 and 800-53A;

d. The Federal Risk and Authorization Management Program security assessment framework;

e. The Center for Internet Security (CIS) Critical Security Controls;

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

g. HITRUST Common Security Framework (CSF);

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

i. Secure Controls Framework; or

j. Other similar industry frameworks or standards; 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, has adopted 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.

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. 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:

(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.

(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 and does not constitute negligence per se.

(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 suit filed on or after the effective date of this act and to any putative class action not certified on or before the effective date of this act.

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