

1                                   A bill to be entitled  
 2           An act relating to cybersecurity incident liability;  
 3           creating s. 768.401, F.S.; providing definitions;  
 4           providing that a county, municipality, other political  
 5           subdivision of the state, covered entity, or third-  
 6           party agent that complies with certain requirements is  
 7           not liable in connection with a cybersecurity  
 8           incident; requiring covered entities and third-party  
 9           agents to adopt revised frameworks, standards, laws,  
 10          or regulations within a specified time period;  
 11          providing that a private cause of action is not  
 12          established; providing that certain failures are not  
 13          evidence of negligence and do not constitute  
 14          negligence per se; specifying that the defendant in  
 15          certain actions has a certain burden of proof;  
 16          providing applicability; providing an effective date.

17  
 18   Be It Enacted by the Legislature of the State of Florida:

19  
 20           Section 1.   Section 768.401, Florida Statutes, is created  
 21   to read:

22           768.401 Limitation on liability for cybersecurity  
 23   incidents.—

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

25           (a) "Covered entity" means a sole proprietorship,

26 partnership, corporation, trust, estate, cooperative,  
 27 association, or other commercial entity.

28 (b) "Third-party agent" means an entity that has been  
 29 contracted to maintain, store, or process personal information  
 30 on behalf of a covered entity.

31 (2) A county or municipality that substantially complies  
 32 with s. 282.3185, and any other political subdivision of the  
 33 state that substantially complies with s. 282.3185 on a  
 34 voluntary basis, is not liable in connection with a  
 35 cybersecurity incident.

36 (3) A covered entity or third-party agent that acquires,  
 37 maintains, stores, processes, or uses personal information is  
 38 not liable in connection with a cybersecurity incident if the  
 39 covered entity or third-party agent does all of the following,  
 40 as applicable:

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

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

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

49 b. NIST special publication 800-171;

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

- 51        d. The Federal Risk and Authorization Management Program  
 52 security assessment framework;
- 53        e. The Center for Internet Security (CIS) Critical  
 54 Security Controls;
- 55        f. The International Organization for  
 56 Standardization/International Electrotechnical Commission 27000-  
 57 series (ISO/IEC 27000) family of standards;
- 58        g. HITRUST Common Security Framework (CSF);
- 59        h. Service Organization Control Type 2 (SOC 2) Framework;
- 60        i. Secure Controls Framework;
- 61        j. Other similar industry frameworks or standards; or  
 62 2. If regulated by the state or Federal Government, or  
 63 both, or if otherwise subject to the requirements of any of the  
 64 following laws and regulations, has adopted a cybersecurity  
 65 program that substantially aligns with the current version of  
 66 the following, as applicable:
- 67        a. The Health Insurance Portability and Accountability Act  
 68 of 1996 security requirements in 45 C.F.R. part 160 and part 164  
 69 subparts A and C.
- 70        b. Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L.  
 71 No. 106-102, as amended.
- 72        c. The Federal Information Security Modernization Act of  
 73 2014, Pub. L. No. 113-283.
- 74        d. The Health Information Technology for Economic and  
 75 Clinical Health Act requirements in 45 C.F.R. parts 160 and 164.

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

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

80 (4) A covered entity's or third-party agent's substantial  
 81 alignment with a framework or standard under subparagraph  
 82 (3)(b)1. or with a law or regulation under subparagraph (3)(b)2.  
 83 may be demonstrated by providing documentation or other evidence  
 84 of an assessment, conducted internally or by a third-party,  
 85 reflecting that the covered entity's or third-party agent's  
 86 cybersecurity program is substantially aligned with the relevant  
 87 frameworks or standards or with the applicable state or federal  
 88 law or regulation. In determining whether a covered entity's or  
 89 third-party agent's cybersecurity program is in substantial  
 90 alignment, all of the following factors must be considered:

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

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

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

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

101 protection from liability.

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

104 (7) Failure of a county, municipality, other political  
 105 subdivision of the state, covered entity, or third-party agent  
 106 to substantially implement a cybersecurity program that is in  
 107 compliance with this section is not evidence of negligence and  
 108 does not constitute negligence per se.

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

114 Section 2. The amendments made by this act apply to any  
 115 suit filed on or after the effective date of this act and to any  
 116 putative class action not certified on or before the effective  
 117 date of this act.

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