

By Senator DiCeglie

18-00891-24

2024658__

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

15 Be It Enacted by the Legislature of the State of Florida:
16

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

19 768.401 Limitation on liability for cybersecurity
20 incidents.—

21 (1) A county or municipality that substantially complies
22 with s. 282.3185 is not liable in connection with a
23 cybersecurity incident.

24 (2) A sole proprietorship, partnership, corporation, trust,
25 estate, cooperative, association, or other commercial entity or
26 third-party agent that acquires, maintains, stores, or uses
27 personal information is not liable in connection with a
28 cybersecurity incident if the entity substantially complies with
29 s. 501.171, if applicable, and has:

18-00891-24

2024658__

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

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

36 2. NIST special publication 800-171.

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

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

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

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

45 (b) If regulated by the state or Federal Government, or
46 both, or if otherwise subject to the requirements of any of the
47 following laws and regulations, substantially aligned its
48 cybersecurity program to the current version of the following,
49 as applicable:

50 1. The Health Insurance Portability and Accountability Act
51 of 1996 security requirements in 45 C.F.R. part 160 and part
52 164, subparts A and C.

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

55 3. The Federal Information Security Modernization Act of
56 2014, Pub. L. No. 113-283.

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

18-00891-24

2024658__

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

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

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

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

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

78 (5) This section does not establish a private cause of
79 action. Failure of a county, municipality, or commercial entity
80 to substantially implement a cybersecurity program that is in
81 compliance with this section is not evidence of negligence and
82 does not constitute negligence per se.

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

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