

By the Committee on Governmental Oversight and Accountability;
and Senator DiCeglie

585-03019-24

2024658c1

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, other political subdivision of the
5 state, commercial entity, or third-party agent that
6 complies with certain requirements is not liable in
7 connection with a cybersecurity incident; requiring
8 certain entities to adopt certain revised frameworks
9 or standards within a specified time period; providing
10 that a private cause of action is not established;
11 providing that certain failures are not evidence of
12 negligence and do not constitute negligence per se;
13 specifying that the defendant in certain actions has a
14 certain burden of proof; providing an effective date.

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

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

20 768.401 Limitation on liability for cybersecurity
21 incidents.—

22 (1) A county or municipality that substantially complies
23 with s. 282.3185, and any other political subdivision of the
24 state that substantially complies with s. 282.3185 on a
25 voluntary basis, is not liable in connection with a
26 cybersecurity incident.

27 (2) A sole proprietorship, partnership, corporation, trust,
28 estate, cooperative, association, or other commercial entity or
29 third-party agent that acquires, maintains, stores, or uses

585-03019-24

2024658c1

30 personal information is not liable in connection with a
31 cybersecurity incident if the entity substantially complies with
32 s. 501.171, if applicable, and has:

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

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

39 2. NIST special publication 800-171.

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

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

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

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

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

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

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

58 3. The Federal Information Security Modernization Act of

585-03019-24

2024658c1

59 2014, Pub. L. No. 113-283.

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

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

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

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

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

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

81 (5) This section does not establish a private cause of
82 action. Failure of a county, municipality, other political
83 subdivision of the state, or commercial entity to substantially
84 implement a cybersecurity program that is in compliance with
85 this section is not evidence of negligence and does not
86 constitute negligence per se.

87 (6) In an action in connection with a cybersecurity

585-03019-24

2024658c1

88 incident, if the defendant is an entity covered by subsection
89 (1) or subsection (2), the defendant has the burden of proof to
90 establish substantial compliance.

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