

**Adopted
COMMITTEE AMENDMENT NO 1 PROPOSED TO**

House Bill No. 1380

BY: Committee

**Amend by striking all after the enacting clause and inserting
in lieu thereof the following:**

13 **SECTION 1.** (1) As used in this act, the following terms
14 shall have the meanings herein ascribed unless the context clearly
15 requires otherwise:

16 (a) "Covered entity" means a sole proprietorship,
17 partnership, company, corporation, trust, estate, cooperative,
18 association, or a financial institution organized, chartered, or
19 holding a license authorizing operation under the laws of this
20 state, another state, or another country, or other commercial
21 entity.

22 (b) "Third-party agent" means an entity that has



23 been contracted to maintain, store, or process personal
24 information on behalf of a covered entity.

25 (2) (a) A county, municipality, county hospital, the state
26 or any of its political subdivisions shall not be liable in
27 connection with a cybersecurity incident if the entity adopts
28 cybersecurity standards that:

29 (i) Safeguard its data, information technology,
30 and information technology resources to ensure availability,
31 confidentiality and integrity; and

32 (ii) Are consistent with generally accepted best
33 practices for cybersecurity, including the National Institute of
34 Standards and Technology Cybersecurity Framework.

35 (b) This statement of immunity shall not be construed
36 to waive any immunity granted to a county, municipality or any
37 other political subdivision under Title 11, Chapter 46,
38 Mississippi Code of 1972.

39 (3) There shall be a rebuttable presumption that a covered
40 entity or third-party agent that acquires, maintains, stores or
41 uses personal information is not liable in connection with a
42 cybersecurity incident if the covered entity or third-party agent,
43 in good faith, substantially complies with reasonable measures to
44 protect and secure data in electronic form containing personal
45 information and has:



46 (a) Adopted a cybersecurity program that substantially
47 aligns with the current version of any standards, guidelines or
48 regulations that implement any of the following:

49 (i) The National Institute of Standards and
50 Technology (NIST) Cybersecurity Framework;

51 (ii) NIST special publication 800-171 or its most
52 current update, revision, or replacement;

53 (iii) NIST special publications 800-53 and 800-53A
54 or their most current update, revision, or replacement;

55 (iv) The Federal Risk and Authorization Management
56 Program security assessment framework;

57 (v) The Center for Internet Security (CIS)
58 Critical Security Controls;

59 (vi) The International Organization for
60 Standardization/International Electrotechnical Commission 27000
61 series (ISO/IEC 27000) family of standards; or

62 (b) 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, substantially aligned its
65 cybersecurity program to the current version of the following, as
66 applicable:

67 (i) The Health Insurance Portability and
68 Accountability Act of 1996 security requirements in 45 CFR part
69 160 and part 164 subparts A and C;



(ii) Title V of the Gramm-Leach-Bliley Act of 1999, Public Law 57 No. 106-102, as amended, and the implementing regulations;

(iii) The Federal Information Security Modernization Act of 2014, Public Law No. 113-283; or

(iv) The Health Information Technology for Economic and Clinical Health Act requirements in 45 CFR parts 160 and 164.

(4) A covered entity's or third-party agent's alignment with a framework or standard under subsection (3)(a) or (b) of this section, 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) The scale and scope of substantial alignment with a standard, law or regulation under subsection (3)(a) or (b) of this section by a covered entity or third-party agent, as applicable, is appropriate if it is based on all of the following factors:

(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.



95 (6) Any commercial entity or third-party agent covered by
96 subsection (3) of this section which substantially complies with a
97 combination of industry-recognized cybersecurity frameworks or
98 standards to gain the presumption against liability pursuant to
99 subsection (3) of this section must, upon the revision of two (2)
100 or more of the frameworks or standards with which the entity
101 complies, adopt the revised frameworks or standards within one (1)
102 year after the latest publication date or latest compliance or
103 effective date stated in the revisions and, if applicable, comply
104 with the Payment Card Industry Data Security Standard (PCI DSS).

105 (7) In an action in connection with a cybersecurity
106 incident, if the defendant is an entity covered by subsection (2)
107 of this section, the plaintiff shall have the initial burden of
108 demonstrating by clear and convincing evidence that the entity was
109 not in substantial compliance with this section.

110 (8) In an action in connection with a cybersecurity
111 incident, if the defendant is an entity under subsection (3) of
112 this section, the defendant has the burden of proof to establish a
113 prima facie case of compliance with industry-recognized
114 cybersecurity frameworks or standards to gain the presumption
115 against liability pursuant to this act. After the defendant meets
116 its initial burden, the burden of proof will then shift to the
117 plaintiff to overcome this presumption against liability by
118 proving by clear and convincing evidence, that the defendant



failed to substantially comply with applicable industry-recognized cybersecurity frameworks or standards.

(9) This act does not establish a private cause of action, including a class action, if a covered entity or third-party agent fails to comply with a provision of this act.

(10) Failure of a county, municipality, county hospital, other political subdivision of the state, or covered entity 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.

(11) A choice of law provision in an agreement that designates this state as the governing law shall apply this act, if applicable, to the fullest extent possible in a civil action brought against a person regardless of whether the civil action is brought in this state or another state.

(12) This section shall apply to any civil action filed on or after July 1, 2025.

SECTION 2. This act shall take effect and be in force from and after July 1, 2025.

Further, amend by striking the title in its entirety and inserting in lieu thereof the following:

AN ACT TO PROVIDE THAT A COUNTY OR MUNICIPALITY AND ANY OTHER POLITICAL SUBDIVISION OF THE STATE SHALL NOT BE LIABLE IN CONNECTION WITH A CYBERSECURITY INCIDENT IF THE ENTITY ADOPTS CERTAIN CYBERSECURITY STANDARDS; TO DEFINE CERTAIN TERMS; TO REQUIRE CYBERSECURITY PROGRAMS TO ALIGN WITH NATIONALLY RECOGNIZED STANDARDS AND THE REQUIREMENTS OF SPECIFIED FEDERAL LAWS; TO



7 PROVIDE A REBUTTABLE PRESUMPTION AGAINST LIABILITY FOR COMMERCIAL
8 ENTITIES THAT ARE IN SUBSTANTIAL COMPLIANCE WITH THIS ACT BY
9 ADOPTING A CYBERSECURITY PROGRAM THAT SUBSTANTIALLY ALIGNS WITH
10 CERTAIN SPECIFIED CYBERSECURITY STANDARDS; AND FOR RELATED
11 PURPOSES.

