

By: Senator(s) Williams, Boyd

To: Judiciary, Division A

SENATE BILL NO. 2471
(As Passed the Senate)

1 AN ACT TO PROVIDE THAT A COUNTY OR MUNICIPALITY AND ANY OTHER
2 POLITICAL SUBDIVISION OF THE STATE SHALL NOT BE LIABLE IN
3 CONNECTION WITH A CYBERSECURITY INCIDENT IF THE ENTITY ADOPTS
4 CERTAIN CYBERSECURITY STANDARDS; TO REQUIRE CYBERSECURITY PROGRAMS
5 TO ALIGN WITH NATIONALLY RECOGNIZED STANDARDS AND THE REQUIREMENTS
6 OF SPECIFIED FEDERAL LAWS; TO PROVIDE A REBUTTABLE PRESUMPTION
7 AGAINST LIABILITY FOR COMMERCIAL ENTITIES THAT ARE IN SUBSTANTIAL
8 COMPLIANCE WITH THIS ACT BY ADOPTING A CYBERSECURITY PROGRAM THAT
9 SUBSTANTIALLY ALIGNS WITH CERTAIN SPECIFIED CYBERSECURITY
10 STANDARDS; AND FOR RELATED PURPOSES.

11 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MISSISSIPPI:

12 **SECTION 1.** (1) As used in this act, the following terms
13 shall have the meanings herein ascribed:

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

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



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

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

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

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

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

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



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

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

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

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

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

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

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

(i) The Health Insurance Portability and Accountability Act of 1996 security requirements in 45 CFR part 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.

(6) Any commercial entity or third-party agent covered by
subsection (3) of this section which substantially complies with a
combination of industry-recognized cybersecurity frameworks or



standards to gain the presumption against liability pursuant to subsection (3) of this section must, upon the revision of two (2) or more of the frameworks or standards with which the entity complies, adopt the revised frameworks or standards within one (1) year after the latest publication date or latest compliance or effective date stated in the revisions and, if applicable, comply with the Payment Card Industry Data Security Standard (PCI DSS).

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

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



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

122 (10) Failure of a county, municipality, county hospital,
123 other political subdivision of the state, or covered entity to
124 substantially implement a cybersecurity program that is in
125 compliance with this section is not evidence of negligence and
126 does not constitute negligence per se.

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

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

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

