

By: Representative Hood

To: Judiciary A; Technology

HOUSE BILL NO. 1380
(As Passed the House)

1 AN ACT TO PROVIDE THAT STATE AND LOCAL GOVERNMENTAL ENTITIES
2 AND CERTAIN COVERED COMMERCIAL ENTITIES ARE NOT LIABLE IN
3 CONNECTION WITH A CYBERSECURITY INCIDENT IF THE ENTITY INVOLVED
4 HAS ADOPTED CERTAIN CYBERSECURITY STANDARDS; TO DEFINE CERTAIN
5 TERMS; TO REQUIRE CYBERSECURITY STANDARDS TO ALIGN WITH
6 NATIONALLY-RECOGNIZED STANDARDS AND THE REQUIREMENTS OF SPECIFIED
7 FEDERAL LAWS; TO CREATE A REBUTTABLE PRESUMPTION AGAINST LIABILITY
8 IN CONNECTION WITH A CYBERSECURITY INCIDENT FOR COMMERCIAL
9 ENTITIES THAT HAVE ADOPTED A CYBERSECURITY PROGRAM THAT
10 SUBSTANTIALLY ALIGNS WITH CERTAIN SPECIFIED CYBERSECURITY
11 STANDARDS IN COMPLIANCE WITH THIS ACT; TO BRING FORWARD SECTION
12 25-53-201, MISSISSIPPI CODE OF 1972, FOR PURPOSES OF POSSIBLE
13 AMENDMENT; AND FOR RELATED PURPOSES.

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

15 **SECTION 1.** (1) As used in this section, the following words
16 and phrases have the meanings ascribed in this subsection unless
17 the context clearly requires otherwise:

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

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



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

26 (2) (a) The state, a county, municipality, county hospital
27 or other political subdivision of the state is not liable in
28 connection with a cybersecurity incident if the entity adopts
29 cybersecurity standards that:

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

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

36 (b) This statement of immunity may not be construed to
37 waive any immunity granted to the state, a county, municipality or
38 other political subdivision of the state under Title 11, Chapter
39 46, Mississippi Code of 1972.

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



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

50 (i) The National Institute of Standards and
51 Technology (NIST) Framework for Improving Critical Infrastructure
52 Cybersecurity and the implementing regulations or publications;

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

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

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

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

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

64 (b) If regulated by the state or federal government, or
65 both, or if otherwise subject to the requirements of any of the
66 following laws and regulations, substantially aligned its
67 cybersecurity program to the current version of the following, as
68 applicable:

69 (i) The Health Insurance Portability and
70 Accountability Act of 1996 security requirements in 45 CFR part
71 160 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 paragraph (a) or (b) of subsection (3) 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 substantially is 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 paragraph (a) or (b) of subsection (3) 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; and



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

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

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

114 (8) In an action in connection with a cybersecurity
115 incident, if the defendant is an entity under subsection (3) of
116 this section, the defendant has the burden of proof to establish a
117 prima facie case of compliance with industry-recognized
118 cybersecurity frameworks or standards to gain the presumption
119 against liability created under this section. If a defendant
120 meets its initial burden, the burden of proof then shifts to the
121 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.

(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 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 applies to 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 is applicable to any suit filed on or after January 1, 2026.

SECTION 2. Section 25-53-201, Mississippi Code of 1972, is brought forward as follows:

25-53-201. (1) There is hereby established the Enterprise Security Program which shall provide for the coordinated oversight of the cybersecurity efforts across all state agencies, including cybersecurity systems, services and the development of policies, standards and guidelines.



(2) The Mississippi Department of Information Technology Services (MDITS), in conjunction with all state agencies, shall provide centralized management and coordination of state policies for the security of data and information technology resources, which such information shall be compiled by MDITS and distributed to each participating state agency. MDITS shall:

(a) Serve as sole authority, within the constraints of this statute, for defining the specific enterprise cybersecurity systems and services to which this statute is applicable;

(b) Acquire and operate enterprise technology solutions to provide services to state agencies when it is determined that such operation will improve the cybersecurity posture in the function of any agency, institution or function of state government as a whole;

(c) Provide oversight of enterprise security policies for state data and information technology (IT) resources including, the following:

(i) Establishing and maintaining the security standards and policies for all state data and IT resources state agencies shall implement to the extent that they apply; and

(ii) Including the defined enterprise security requirements as minimum requirements in the specifications for solicitation of state contracts for procuring data and information technology systems and services;



171 (d) Adhere to all policies, standards and guidelines in
172 the management of technology infrastructure supporting the state
173 data centers, telecommunications networks and backup facilities;

174 (e) Coordinate and promote efficiency and security with
175 all applicable laws and regulations in the acquisition, operation
176 and maintenance of state data, cybersecurity systems and services
177 used by agencies of the state;

178 (f) Manage, plan and coordinate all enterprise
179 cybersecurity systems under the jurisdiction of the state;

180 (g) Develop, in conjunction with agencies of the state,
181 coordinated enterprise cybersecurity systems and services for all
182 state agencies;

183 (h) Provide ongoing analysis of enterprise
184 cybersecurity systems and services costs, facilities and systems
185 within state government;

186 (i) Develop policies, procedures and long-range plans
187 for the use of enterprise cybersecurity systems and services;

188 (j) Form an advisory council of information security
189 officers from each state agency to plan, develop and implement
190 cybersecurity initiatives;

191 (k) Coordinate the activities of the advisory council
192 to provide education and awareness, identify cybersecurity-related
193 issues, set future direction for cybersecurity plans and policy,
194 and provide a forum for interagency communications regarding
195 cybersecurity;



(1) Charge respective user agencies on a reimbursement basis for their proportionate cost of the installation, maintenance and operation of the cybersecurity systems and services; and

(m) Require cooperative utilization of cybersecurity systems and services by aggregating users.

(3) Each state agency's executive director or agency head shall:

(a) Be solely responsible for the security of all data and IT resources under its purview, irrespective of the location of the data or resources. Locations include data residing:

(i) At agency sites;

(ii) On agency real property and tangible and intangible assets;

(iii) On infrastructure in the State Data Centers;

(iv) At a third-party location;

(v) In transit between locations;

(b) Ensure that an agency-wide security program is in place;

(c) Designate an information security officer to administer the agency's security program;

(d) Ensure the agency adheres to the requirements established by the Enterprise Security Program, to the extent that they apply;



220 (e) Participate in all Enterprise Security Program
221 initiatives and services in lieu of deploying duplicate services
222 specific to the agency;

223 (f) Develop, implement and maintain written agency
224 policies and procedures to ensure the security of data and IT
225 resources. The agency policies and procedures are confidential
226 information and exempt from public inspection, except that the
227 information must be available to the Office of the State Auditor
228 in performing auditing duties;

229 (g) Implement policies and standards to ensure that all
230 of the agency's data and IT resources are maintained in compliance
231 with state and federal laws and regulations, to the extent that
232 they apply;

233 (h) Implement appropriate cost-effective safeguards to
234 reduce, eliminate or recover from identified threats to data and
235 IT resources;

236 (i) Ensure that internal assessments of the security
237 program are conducted. The results of the internal assessments
238 are confidential and exempt from public inspection, except that
239 the information must be available to the Office of the State
240 Auditor in performing auditing duties;

241 (j) Include all appropriate cybersecurity requirements
242 in the specifications for the agency's solicitation of state
243 contracts for procuring data and information technology systems
244 and services;



(k) Include a general description of the security program and future plans for ensuring security of data in the agency long-range information technology plan;

(l) Participate in annual information security training designed specifically for the executive director or agency head to ensure that such individual has an understanding of:

(i) The information and information systems that support the operations and assets of the agency;

(ii) The potential impact of common types of cyber-attacks and data breaches on the agency's operations and assets;

(iii) How cyber-attacks and data breaches on the agency's operations and assets could impact the operations and assets of other state agencies on the Enterprise State Network;

(iv) How cyber-attacks and data breaches occur;

(v) Steps to be undertaken by the executive director or agency head and agency employees to protect their information and information systems; and

(vi) The annual reporting requirements required of the executive director or agency head.

(4) The Mississippi Department of Information Technology Services shall evaluate the Enterprise Security Program. Such evaluation shall include the following factors:

(a) Whether the Enterprise Security Program incorporates nationwide best practices;



(b) Whether opportunities exist to centralize and coordinate oversight of cybersecurity efforts across all state agencies;

(c) A review of the minimum enterprise security requirements that must be incorporated in solicitations for state contracts for procuring data and information technology systems and services; and

(d) Whether opportunities exist to expand the Enterprise Security Program, including providing oversight of cybersecurity efforts of those governing authorities as defined in Section 25-53-3(f).

In performing such evaluation, the Mississippi Department of Information Technology Services may retain experts. This evaluation shall be completed by November 1, 2023. All records in connection with this evaluation shall be exempt from the Mississippi Public Records Act of 1983, pursuant to Section 25-61-11.2(f) and (k).

(5) For the purpose of this subsection, the following words shall have the meanings ascribed herein, unless the context clearly indicates otherwise:

(a) "Cyberattack" shall mean any attempt to gain illegal access, including any data breach, to a computer, computer system or computer network for purposes of causing damage, disruption or harm.



294 (b) "Ransomware" shall mean a computer contaminant or
295 lock placed or introduced without authorization into a computer,
296 computer system or computer network that restricts access by an
297 authorized person to the computer, computer system, computer
298 network or any data therein under circumstances in which the
299 person responsible for the placement or introduction of the
300 ransomware demands payment of money or other consideration to
301 remove the computer contaminant, restore access to the computer,
302 computer system, computer network or data, or otherwise remediate
303 the impact of the computer contaminant or lock.

304 (c) From and after July 1, 2023, all state agencies
305 shall notify the Mississippi Department of Information Technology
306 Services of any cyberattack or demand for payment as a result of
307 ransomware no later than the close of the next business day
308 following the discovery of such cyberattack or demand. The
309 Mississippi Department of Information Technology Services shall
310 develop a reporting format to be utilized by state agencies to
311 provide such notification. The Mississippi Department of
312 Information Technology Services shall periodically analyze all
313 such reports and attempt to identify any patterns or weaknesses in
314 the state's cybersecurity efforts. Such reports shall be exempt
315 from the Mississippi Public Records Act of 1983, pursuant to
316 Section 25-61-11.2(j).



317 **SECTION 3.** This act shall take effect and be in force from
318 and after January 1, 2026, and shall stand repealed on December
319 31, 2025.

