To: Technology

By: Senator(s) DeLano

COMMITTEE SUBSTITUTE FOR SENATE BILL NO. 2717

AN ACT TO AMEND SECTION 25-53-201, MISSISSIPPI CODE OF 1972, TO PROVIDE THAT THE MISSISSIPPI DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES SHALL EVALUATE THE OPPORTUNITIES FOR EXPANDING THE ENTERPRISE SECURITY PROGRAM AND THE COORDINATED OVERSIGHT OF 5 CYBERSECURITY EFFORTS TO INCLUDE THOSE GOVERNING AUTHORITIES DEFINED IN SECTION 25-53-3(F); TO REQUIRE THE DEPARTMENT TO 7 DEVELOP A REPORT ON THESE OPPORTUNITIES AND TO PRESENT THE REPORT TO THE CHAIRMEN OF THE SENATE AND HOUSE OF REPRESENTATIVES 8 9 ACCOUNTABILITY, EFFICIENCY, TRANSPARENCY COMMITTEES, ATTORNEY GENERAL AND THE CHAIRMAN OF THE SENATE TECHNOLOGY COMMITTEE BY 10 11 NOVEMBER 1, 2023; TO PROVIDE THAT FROM AND AFTER JULY 1, 2023, ALL 12 STATE AGENCIES AND GOVERNING AUTHORITIES AS DEFINED IN SECTION 25-53-3 SHALL REPORT TO THE MISSISSIPPI DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES ANY DEMAND FOR PAYMENT OR ANY PAYMENT MADE AS 14 1.5 A RESULT OF RANSOMWARE; TO DEFINE RANSOMWARE; TO REQUIRE THESE 16 AGENCIES AND AUTHORITIES TO REPORT THIS INFORMATION NO LATER THAN 17 THE NEXT BUSINESS DAY UPON DISCOVERY OF THE RANSOMWARE; TO REQUIRE 18 THE DEPARTMENT TO RECORD ALL INFORMATION SUBMITTED FROM THESE 19 AGENCIES AND AUTHORITIES AND DEVELOP A REPORT ON THIS INFORMATION; 20 TO REQUIRE THE DEPARTMENT TO PRESENT THIS REPORT TO THE LIEUTENANT 21 GOVERNOR, SPEAKER OF THE HOUSE, ATTORNEY GENERAL, CHAIRMEN OF THE 22 SENATE AND HOUSE OF REPRESENTATIVES ACCOUNTABILITY, EFFICIENCY, 23 TRANSPARENCY COMMITTEES AND THE CHAIRMAN OF THE SENATE TECHNOLOGY 24 COMMITTEE; TO REQUIRE THE DEPARTMENT TO PRESENT A YEARLY SUMMARY 25 OF ALL RANSOMWARE INCIDENTS BY NOVEMBER 1 OF EACH YEAR TO THE 26 LIEUTENANT GOVERNOR, SPEAKER OF THE HOUSE, CHAIRMEN OF THE SENATE 27 AND HOUSE OF REPRESENTATIVES ACCOUNTABILITY, EFFICIENCY, 28 TRANSPARENCY COMMITTEES AND THE CHAIRMAN OF THE SENATE TECHNOLOGY 29 COMMITTEE; AND FOR RELATED PURPOSES.

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

30

- 31 **SECTION 1.** Section 25-53-201, Mississippi Code of 1972, is
- 32 amended as follows:
- 33 25-53-201. (1) There is hereby established the Enterprise
- 34 Security Program which shall provide for the coordinated oversight
- 35 of the cybersecurity efforts across all state agencies, including
- 36 cybersecurity systems, services and the development of policies,
- 37 standards and guidelines.
- 38 (2) The Mississippi Department of Information Technology
- 39 Services (MDITS), in conjunction with all state agencies, shall
- 40 provide centralized management and coordination of state policies
- 41 for the security of data and information technology resources,
- 42 which such information shall be compiled by MDITS and distributed
- 43 to each participating state agency. MDITS shall:
- 44 (a) Serve as sole authority, within the constraints of
- 45 this statute, for defining the specific enterprise cybersecurity
- 46 systems and services to which this statute is applicable;
- 47 (b) Acquire and operate enterprise technology solutions
- 48 to provide services to state agencies when it is determined that
- 49 such operation will improve the cybersecurity posture in the
- 50 function of any agency, institution or function of state
- 51 government as a whole;
- 52 (c) Provide oversight of enterprise security policies
- 53 for state data and information technology (IT) resources
- 54 including, the following:

55 (i)	Establishing an	nd maintaining	the security
--------	-----------------	----------------	--------------

56 standards and policies for all state data and IT resources state

- 57 agencies shall implement to the extent that they apply; and
- 58 (ii) Including the defined enterprise security
- 59 requirements as minimum requirements in the specifications for
- 60 solicitation of state contracts for procuring data and information
- 61 technology systems and services;
- 62 (d) Adhere to all policies, standards and guidelines in
- 63 the management of technology infrastructure supporting the state
- 64 data centers, telecommunications networks and backup facilities;
- 65 (e) Coordinate and promote efficiency and security with
- 66 all applicable laws and regulations in the acquisition, operation
- 67 and maintenance of state data, cybersecurity systems and services
- 68 used by agencies of the state;
- (f) Manage, plan and coordinate all enterprise
- 70 cybersecurity systems under the jurisdiction of the state;
- 71 (q) Develop, in conjunction with agencies of the state,
- 72 coordinated enterprise cybersecurity systems and services for all
- 73 state agencies;
- 74 (h) Provide ongoing analysis of enterprise
- 75 cybersecurity systems and services costs, facilities and systems
- 76 within state government;
- 77 (i) Develop policies, procedures and long-range plans
- 78 for the use of enterprise cybersecurity systems and services;

	1
80	officers from each state agency to plan, develop and implement
81	cybersecurity initiatives;
82	(k) Coordinate the activities of the advisory council
83	to provide education and awareness, identify cybersecurity-related
84	issues, set future direction for cybersecurity plans and policy,
85	and provide a forum for interagency communications regarding
86	cybersecurity;
87	(1) Charge respective user agencies on a reimbursement
88	basis for their proportionate cost of the installation,
89	maintenance and operation of the cybersecurity systems and
90	services; and
91	(m) Require cooperative utilization of cybersecurity
92	systems and services by aggregating users.
93	(3) Each state agency's executive director or agency head
94	shall:
95	(a) Be solely responsible for the security of all data
96	and IT resources under its purview, irrespective of the location
97	of the data or resources. Locations include data residing:
98	(i) At agency sites;
99	(ii) On agency real property and tangible and

(j) Form an advisory council of information security

(iv) At a third-party location;

(v) In transit between locations;

(iii) On infrastructure in the State Data Centers;

intangible assets;

100

101

102

103

79

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

- 106 (c) Designate an information security officer to 107 administer the agency's security program;
- 108 (d) Ensure the agency adheres to the requirements
 109 established by the Enterprise Security Program, to the extent that
 110 they apply;
- (e) Participate in all Enterprise Security Program
 initiatives and services in lieu of deploying duplicate services
 specific to the agency;
- (f) Develop, implement and maintain written agency
 policies and procedures to ensure the security of data and IT
 resources. The agency policies and procedures are confidential
 information and exempt from public inspection, except that the
 information must be available to the Office of the State Auditor
 in performing auditing duties;
- 120 (g) Implement policies and standards to ensure that all
 121 of the agency's data and IT resources are maintained in compliance
 122 with state and federal laws and regulations, to the extent that
 123 they apply;
- (h) Implement appropriate cost-effective safeguards to reduce, eliminate or recover from identified threats to data and IT resources;
- 127 (i) Ensure that internal assessments of the security
 128 program are conducted. The results of the internal assessments

129	are	confidential	and	exemp	t from	pub.	lic .	inspect	ion,	exc	cept	that
130	the	information	must	be av	ailable	e to	the	Office	of	the	Stat	te

131 Auditor in performing auditing duties;

- (j) Include all appropriate cybersecurity requirements in the specifications for the agency's solicitation of state contracts for procuring data and information technology systems and services;
- 136 (k) Include a general description of the security
 137 program and future plans for ensuring security of data in the
 138 agency long-range information technology plan;
- (1) Participate in annual information security training
 designed specifically for the executive director or agency head to
 ensure that such individual has an understanding of:
- 142 (i) The information and information systems that 143 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;
- 147 (iii) How cyber-attacks and data breaches on the 148 agency's operations and assets could impact the operations and 149 assets of other state agencies on the Enterprise State Network;
- 150 (iv) How cyber-attacks and data breaches occur;
- 151 (v) Steps to be undertaken by the executive 152 director or agency head and agency employees to protect their
- 153 information and information systems; and

154	(vi) The annual reporting requirements required of
155	the executive director or agency head.
156	(4) The Mississippi Department of Information Technology
157	Services shall evaluate the Enterprise Security Program. Such
158	evaluation shall include the following factors:
159	(a) Whether the Enterprise Security Program
160	incorporates nationwide best practices;
161	(b) Whether opportunities exist to centralize and
162	coordinate oversight of cybersecurity efforts across all state
163	agencies;
164	(c) A review of the minimum enterprise security
165	requirements that must be incorporated in solicitations for state
166	contracts for procuring data and information technology systems
167	and services; and
168	(d) Whether opportunities exist to expand the
169	Enterprise Security Program, including providing oversight of
170	cybersecurity efforts of those governing authorities as defined in
171	Section 25-53-3(f).
172	In performing such evaluation, the Mississippi Department of
173	Information Technology Services may retain experts. This
174	evaluation shall be completed by November 1, 2023. All records in
175	connection with this evaluation shall be exempt from the
176	Mississippi Public Records Act of 1983, pursuant to Section
177	25-61-11.2(f) and (k).

178	(5) For the purpose of this subsection, the following words
179	shall have the meanings ascribed herein, unless the context
180	<pre>clearly indicates otherwise:</pre>
181	(a) "Cyberattack" shall mean any attempt to gain
182	illegal access, including any data breach, to a computer, computer
183	system or computer network for purposes of causing damage,
184	disruption or harm.
185	(b) "Ransomware" shall mean a computer contaminant or
186	lock placed or introduced without authorization into a computer,
187	computer system or computer network that restricts access by an
188	authorized person to the computer, computer system, computer
189	network or any data therein under circumstances in which the
190	person responsible for the placement or introduction of the
191	ransomware demands payment of money or other consideration to
192	remove the computer contaminant, restore access to the computer,
193	computer system, computer network or data, or otherwise remediate
194	the impact of the computer contaminant or lock.
195	(c) From and after July 1, 2023, all state agencies
196	shall notify the Mississippi Department of Information Technology
197	Services of any cyberattack or demand for payment as a result of
198	ransomware no later than the close of the next business day
199	following the discovery of such cyberattack or demand. The
200	Mississippi Department of Information Technology Services shall
201	develop a reporting format to be utilized by state agencies to
202	provide such notification. The Mississippi Department of

203	Information Technology Services shall periodically analyze all
204	such reports and attempt to identify any patterns or weaknesses in
205	the state's cybersecurity efforts. Such reports shall be exempt
206	from the Mississippi Public Records Act of 1983, pursuant to
207	Section 25-61-11.2(j).
208	SECTION 2. This act shall take effect and be in force from
209	and after July 1, 2023.

