

By: Senator(s) DeLano, Williams

To: Technology

COMMITTEE SUBSTITUTE
FOR
SENATE BILL NO. 2530

1 AN ACT TO AMEND SECTION 25-53-201, MISSISSIPPI CODE OF 1972,
2 TO PROVIDE THAT THE MISSISSIPPI DEPARTMENT OF INFORMATION
3 TECHNOLOGY SERVICES SHALL EVALUATE THE OPPORTUNITIES FOR EXPANDING
4 THE ENTERPRISE SECURITY PROGRAM AND THE COORDINATED OVERSIGHT OF
5 CYBERSECURITY EFFORTS TO INCLUDE THOSE GOVERNING AUTHORITIES
6 DEFINED IN SECTION 25-53-3(F); TO REQUIRE THE DEPARTMENT TO
7 DEVELOP A REPORT ON THESE OPPORTUNITIES AND TO PRESENT THE REPORT
8 TO THE CHAIRMEN OF THE SENATE AND HOUSE OF REPRESENTATIVES
9 ACCOUNTABILITY, EFFICIENCY, TRANSPARENCY COMMITTEES AND THE
10 CHAIRMAN OF THE SENATE TECHNOLOGY COMMITTEE BY NOVEMBER 1, 2022;
11 TO PROVIDE THAT FROM AND AFTER JULY 1, 2022, ALL STATE AGENCIES
12 AND GOVERNING AUTHORITIES AS DEFINED IN SECTION 25-53-3 SHALL
13 REPORT TO THE MISSISSIPPI DEPARTMENT OF INFORMATION TECHNOLOGY
14 SERVICES ANY DEMAND FOR PAYMENT OR ANY PAYMENT MADE AS A RESULT OF
15 RANSOMWARE; TO DEFINE RANSOMWARE; TO REQUIRE THESE AGENCIES AND
16 AUTHORITIES TO REPORT THIS INFORMATION WITHIN 24 HOURS OF
17 DISCOVERY OF THE RANSOMWARE; TO REQUIRE THE DEPARTMENT TO RECORD
18 ALL INFORMATION SUBMITTED FROM THESE AGENCIES AND AUTHORITIES AND
19 DEVELOP A REPORT ON THIS INFORMATION WITHIN 48 HOURS OF DISCOVERY;
20 TO REQUIRE THE DEPARTMENT TO PRESENT THIS REPORT TO THE LIEUTENANT
21 GOVERNOR, SPEAKER OF THE HOUSE, CHAIRMEN OF THE SENATE AND HOUSE
22 OF REPRESENTATIVES ACCOUNTABILITY, EFFICIENCY, TRANSPARENCY
23 COMMITTEES AND THE CHAIRMAN OF THE SENATE TECHNOLOGY COMMITTEE; TO
24 REQUIRE THE DEPARTMENT TO PRESENT A YEARLY SUMMARY OF ALL
25 RANSOMWARE INCIDENTS BY NOVEMBER 1 OF EACH YEAR TO THE LIEUTENANT
26 GOVERNOR, SPEAKER OF THE HOUSE, CHAIRMEN OF THE SENATE AND HOUSE
27 OF REPRESENTATIVES ACCOUNTABILITY, EFFICIENCY, TRANSPARENCY
28 COMMITTEES AND THE CHAIRMAN OF THE SENATE TECHNOLOGY COMMITTEE;
29 AND FOR RELATED PURPOSES.

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



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 and 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;

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

71 (g) 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;



79 (j) Form an advisory council of information security
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 (l) 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
100 intangible assets;

101 (iii) On infrastructure in the State Data Centers;

102 (iv) At a third-party location;

103 (v) In transit between locations;



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;

111 (e) Participate in all Enterprise Security Program
112 initiatives and services in lieu of deploying duplicate services
113 specific to the agency;

114 (f) Develop, implement and maintain written agency
115 policies and procedures to ensure the security of data and IT
116 resources. The agency policies and procedures are confidential
117 information and exempt from public inspection, except that the
118 information must be available to the Office of the State Auditor
119 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;

124 (h) Implement appropriate cost-effective safeguards to
125 reduce, eliminate or recover from identified threats to data and
126 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 exempt from public inspection, except that
130 the information must be available to the Office of the State
131 Auditor in performing auditing duties;

132 (j) Include all appropriate cybersecurity requirements
133 in the specifications for the agency's solicitation of state
134 contracts for procuring data and information technology systems
135 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;

139 (l) Participate in annual information security training
140 designed specifically for the executive director or agency head to
141 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;

144 (ii) The potential impact of common types of
145 cyber-attacks and data breaches on the agency's operations and
146 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 opportunities for expanding the
158 Enterprise Security Program and the coordinated oversight of
159 cybersecurity efforts to include those governing authorities as
160 defined in Section 25-53-3(f). The Mississippi Department of
161 Information Technology Services shall develop a report on these
162 opportunities. The Mississippi Department of Information
163 Technology Services shall present this report to the Chairmen of
164 the Senate and House of Representatives Accountability,
165 Efficiency, Transparency Committees, Attorney General and the
166 Chairman of the Senate Technology Committee by November 1, 2022.

167 (5) From and after July 1, 2022, all state agencies and
168 governing authorities as defined in Section 25-53-3 shall report
169 to the Mississippi Department of Information Technology Services
170 any demand for payment or any payment made as a result of
171 ransomware. These agencies and authorities shall report this
172 information within twenty-four (24) hours of discovery of the
173 ransomware. The Mississippi Department of Information Technology
174 Services shall record all information submitted from these
175 agencies and authorities and develop a report on this information
176 within forty-eight (48) hours of discovery. The Mississippi
177 Department of Information Technology Services shall present this
178 report to the Lieutenant Governor, Speaker of the House, Attorney



179 General, Chairmen of the Senate and House of Representatives
180 Accountability, Efficiency, Transparency Committees and the
181 Chairman of the Senate Technology Committee. By November 1 of
182 each year, the Mississippi Department of Information Technology
183 Services shall provide a yearly summary of all ransomware
184 incidents to the Lieutenant Governor, Speaker of the House,
185 Chairmen of the Senate and House of Representatives
186 Accountability, Efficiency, Transparency Committees and the
187 Chairman of the Senate Technology Committee. For the purpose of
188 this subsection, "ransomware" shall mean a computer contaminant,
189 or lock placed or introduced without authorization into a
190 computer, computer system, or computer network that restricts
191 access by an authorized person to the computer, computer system,
192 computer network, or any data therein under circumstances in which
193 the person responsible for the placement or introduction of the
194 ransomware demands payment of money or other consideration to
195 remove the computer contaminant, restore access to the computer,
196 computer system, computer network, or data, or otherwise remediate
197 the impact of the computer contaminant or lock.

198 **SECTION 2.** This act shall take effect and be in force from
199 and after July 1, 2022.

