

By: Senator(s) DeLano, Williams

To: Technology

SENATE BILL NO. 2530

1 AN ACT TO BRING FORWARD SECTION 25-53-201, MISSISSIPPI CODE
2 OF 1972, WHICH ESTABLISHES THE STATE ENTERPRISE SECURITY PROGRAM,
3 FOR PURPOSE OF POSSIBLE AMENDMENT; AND FOR RELATED PURPOSES.

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

5 **SECTION 1.** Section 25-53-201, Mississippi Code of 1972, is
6 brought forward as follows:

7 25-53-201. (1) There is hereby established the Enterprise
8 Security Program which shall provide for the coordinated oversight
9 of the cybersecurity efforts across all state agencies, including
10 cybersecurity systems, services and the development of policies,
11 standards and guidelines.

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



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

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

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

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

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

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

39 (e) Coordinate and promote efficiency and security with
40 all applicable laws and regulations in the acquisition, operation
41 and maintenance of state data, cybersecurity systems and services
42 used by agencies of the state;



- 43 (f) Manage, plan and coordinate all enterprise
44 cybersecurity systems under the jurisdiction of the state;
- 45 (g) Develop, in conjunction with agencies of the state,
46 coordinated enterprise cybersecurity systems and services for all
47 state agencies;
- 48 (h) Provide ongoing analysis of enterprise
49 cybersecurity systems and services costs, facilities and systems
50 within state government;
- 51 (i) Develop policies, procedures and long-range plans
52 for the use of enterprise cybersecurity systems and services;
- 53 (j) Form an advisory council of information security
54 officers from each state agency to plan, develop and implement
55 cybersecurity initiatives;
- 56 (k) Coordinate the activities of the advisory council
57 to provide education and awareness, identify cybersecurity-related
58 issues, set future direction for cybersecurity plans and policy,
59 and provide a forum for interagency communications regarding
60 cybersecurity;
- 61 (l) Charge respective user agencies on a reimbursement
62 basis for their proportionate cost of the installation,
63 maintenance and operation of the cybersecurity systems and
64 services; and
- 65 (m) Require cooperative utilization of cybersecurity
66 systems and services by aggregating users.



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

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

72 (i) At agency sites;

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

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

76 (iv) At a third party location;

77 (v) In transit between locations;

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

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

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

85 (e) Participate in all Enterprise Security Program
86 initiatives and services in lieu of deploying duplicate services
87 specific to the agency;

88 (f) Develop, implement and maintain written agency
89 policies and procedures to ensure the security of data and IT
90 resources. The agency policies and procedures are confidential
91 information and exempt from public inspection, except that the



92 information must be available to the Office of the State Auditor
93 in performing auditing duties;

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

98 (h) Implement appropriate cost-effective safeguards to
99 reduce, eliminate or recover from identified threats to data and
100 IT resources;

101 (i) Ensure that internal assessments of the security
102 program are conducted. The results of the internal assessments
103 are confidential and exempt from public inspection, except that
104 the information must be available to the Office of the State
105 Auditor in performing auditing duties;

106 (j) Include all appropriate cybersecurity requirements
107 in the specifications for the agency's solicitation of state
108 contracts for procuring data and information technology systems
109 and services;

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

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



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

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

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

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

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

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

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

