

By: Representatives DeLano, Staples, Sykes

To: Technology

COMMITTEE SUBSTITUTE  
FOR  
HOUSE BILL NO. 999

1 AN ACT TO CREATE NEW SECTION 25-53-201, MISSISSIPPI CODE OF  
2 1972, TO ESTABLISH THE ENTERPRISE SECURITY PROGRAM WHICH SHALL  
3 PROVIDE FOR THE COORDINATED OVERSIGHT OF THE CYBERSECURITY EFFORTS  
4 ACROSS ALL STATE AGENCIES; TO REQUIRE THE MISSISSIPPI DEPARTMENT  
5 OF INFORMATION TECHNOLOGY SERVICES TO PROVIDE CENTRALIZED  
6 MANAGEMENT AND COORDINATION OF STATE POLICIES FOR THE SECURITY OF  
7 DATA AND INFORMATION TECHNOLOGY RESOURCES; TO PRESCRIBE THE  
8 RESPONSIBILITIES OF MDITS WITH REGARD TO ADMINISTERING THE  
9 PROVISIONS OF THE PROGRAM; TO PRESCRIBE THE RESPONSIBILITIES OF  
10 EACH STATE AGENCY'S EXECUTIVE DIRECTOR OR AGENCY HEAD WITH REGARDS  
11 TO INSURING THE PROTECTION OF AGENCY AND EMPLOYEE DATA AND  
12 INFORMATION SYSTEMS; AND FOR RELATED PURPOSES.

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

14 **SECTION 1.** The following shall be codified as Section  
15 25-53-201, Mississippi Code of 1972:

16 25-53-201. (1) There is hereby established the Enterprise  
17 Security Program which shall provide for the coordinated oversight  
18 of the cybersecurity efforts across all state agencies, including  
19 cybersecurity systems, services and the development of policies,  
20 standards and guidelines.

21 (2) The Mississippi Department of Information Technology  
22 Services (MDITS), in conjunction with all state agencies, shall  
23 provide centralized management and coordination of state policies



24 for the security of data and information technology resources,  
25 which such information shall be compiled by MDITS and distributed  
26 to each participating state agency. MDITS shall:

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

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

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

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

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

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



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

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

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

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

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

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

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

(l) Charge respective user agencies on a reimbursement basis for their proportionate cost of the installation,



72 maintenance and operation of the cybersecurity systems and  
73 services; and

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

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

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

81 (i) At agency sites;

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

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

85 (iv) At a third party location;

86 (v) In transit between locations;

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

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

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

94 (e) Participate in all Enterprise Security Program  
95 initiatives and services in lieu of deploying duplicate services  
96 specific to the agency;



97                   (f) Develop, implement and maintain written agency  
98 policies and procedures to ensure the security of data and IT  
99 resources. The agency policies and procedures are confidential  
100 information and exempt from public inspection, except that the  
101 information must be available to the Office of the State Auditor  
102 in performing auditing duties;

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

107                   (h) Implement appropriate cost-effective safeguards to  
108 reduce, eliminate or recover from identified threats to data and  
109 IT resources;

110                   (i) Ensure that internal assessments of the security  
111 program are conducted. The results of the internal assessments  
112 are confidential and exempt from public inspection, except that  
113 the information must be available to the Office of the State  
114 Auditor in performing auditing duties;

115                   (j) Include all appropriate cybersecurity requirements  
116 in the specifications for the agency's solicitation of state  
117 contracts for procuring data and information technology systems  
118 and services;

119                   (k) Include a general description of the security  
120 program and future plans for ensuring security of data in the  
121 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:

(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.

**SECTION 2.** This act shall take effect and be in force from and after July 1, 2017.

