MISSISSIPPI LEGISLATURE REGULAR SESSION 2024

By: Senator(s) Williams

To: Technology

SENATE BILL NO. 2703

AN ACT TO AMEND SECTION 25-53-201, MISSISSIPPI CODE OF 1972, TO REQUIRE STATE AGENCIES TO REPORT RANSOMWARE INCIDENTS TO THE ENTERPRISE SECURITY PROGRAM AND THE MISSISSIPPI DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES; TO DEFINE TERMS; TO REQUIRE THAT REPORTS NOTE THE SEVERITY LEVEL OF THE INCIDENT ACCORDING TO THE LEVELS DEFINED BY THE NATIONAL CYBER INCIDENT RESPONSE PLAN OF THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY; TO PROHIBIT STATE AGENCIES FROM PAYING OR OTHERWISE COMPLYING WITH A RANSOM DEMAND; TO ESTABLISH MINIMUM REPORTING REQUIREMENTS FOR STATE AGENCIES; TO REQUIRE THAT REPORTS BE MADE WITHIN CERTAIN TIME RESTRAINTS ACCORDING TO SEVERITY LEVEL; TO REQUIRE THAT THE ENTERPRISE SECURITY PROGRAM MAKE A REPORT TO THE LIEUTENANT GOVERNOR, THE SPEAKER OF THE HOUSE OF REPRESENTATIVES, AND THE CHAIRMEN OF THE LEGISLATIVE TECHNOLOGY COMMITTEES ON A QUARTERLY BASIS; AND FOR RELATED PURPOSES.

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

SECTION 1. Section 25-53-201, Mississippi Code of 1972, is amended 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;

(d) Adhere to all policies, standards and guidelines in the management of technology infrastructure supporting the state 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, 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;

(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;

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

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

(i) Ensure that internal assessments of the security program are conducted. The results of the internal assessments are confidential and exempt from public inspection, except that the information must be available to the Office of the State 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;

(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.

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

(c) "Ransomware incident" means a malicious cyberattack in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies or otherwise renders unavailable a state agency's data, and thereafter, the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

(d) The level of security of the cyberattack is defined by the National Cyber Incident Response Plan of the United States Department of Homeland Security as follows:

(i) Level 5 is an emergency-level incident within the specified jurisdiction that poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local government security; or the lives of the country's, state's, or local government's residents;

(ii) Level 4 is a severe-level incident that is likely to result in a significant impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; or civil liberties;

(iii) Level 3 is a high-level incident that is likely to result in a demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; civil liberties; or public confidence;

(iv) Level 2 is a medium-level incident that may impact public health or safety; national, state or local security; economic security; civil liberties; or public confidence;

(v) Level 1 is a low-level incident that is unlikely to impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence.

(* * *e) A state agency experiencing a ransomware incident shall not pay or otherwise comply with a ransom demand.

(f) From and after July 1, 2023, all state agencies shall notify the Mississippi Department of Information Technology Services of any cyberattack or * * * ransomware incident no later than the close of the next business day following the discovery of such cyberattack or * * * ransomware incident. The Mississippi Department of Information Technology Services shall develop a reporting format to be utilized by state agencies to provide such

notification. The Mississippi Department of Information Technology Services shall periodically analyze all such reports and attempt to identify any patterns or weaknesses in the state's cybersecurity efforts. Such reports shall be exempt from the Mississippi Public Records Act of 1983, pursuant to Section 25-61-11.2(j).

(g) The cyberattack or ransomware incident reporting format shall specify the information that must be reported by a state agency following a cyberattack or ransomware incident, which, at a minimum, must include the following:

(i) A summary of the facts surrounding the cyberattack or ransomware incident;

(ii) The date on which the state agency most recently backed up its data, the physical location of the backup, if the backup was affected, and if the backup was created using cloud computing;

(iii) The types of data compromised by the cyberattack or ransomware incident;

(iv) The estimated fiscal impact of the cyberattack or ransomware incident; and

(v) In the case of a ransomware incident, the details of the ransom demanded.

(h) (i) A state agency shall report all ransomware incidents and any cyberattack determined by the state agency to be of severity level 3, 4 or 5 to the Enterprise Security Program and

the Mississippi Department of Information Technology Services as soon as possible but no later than forty-eight (48) hours after discovery of a cyberattack and no later than twelve (12) hours after discovery of a ransomware incident. The report must contain the information required in paragraph (f) of this subsection.

(ii) The Enterprise Security Program shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4 or 5 incident as soon as possible but no later than twelve (12) hours after receiving a state agency's incident report. The notification shall include a high-level description of the incident and the likely effects.

(i) A state agency shall report a cyberattack or ransomware incident determined by the state agency to be of severity level 1 or 2 to the Enterprise Security Program of the Mississippi Department of Information Technology Services as soon as possible. The report shall contain the information required in paragraph (f) of this subsection.

(j) The Enterprise Security Program shall provide a consolidated incident report on a quarterly basis to the Lieutenant Governor as President of the Senate, the Speaker of the House of Representatives, and the Chairmen of the Legislative Technology Committees.

SECTION 2. This act shall take effect and be in force from and after July 1, 2024.