By: Jetton H.B. No. 2494

A BILL TO BE ENTITLED

AN ACT

relating to information security officers and network threat detection and response for state agencies.

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

SECTION 1. Section 2054.133(b), Government Code, is amended to read as follows:

(b) In developing the plan, the state agency shall:

(1) consider any vulnerability report prepared under Section 2054.077 for the agency;

(2) incorporate the network security services provided by the department to the agency under Chapter 2059;

(3) identify and define the responsibilities of agency staff who produce, access, use, or serve as custodians of the agency's information;

(4) identify risk management and other measures taken to protect the agency's information from unauthorized access, disclosure, modification, or destruction;

(5) include:

(A) the best practices for information security developed by the department; or

(B) a written explanation of why the best practices are not sufficient for the agency's security; [~~and~~]

(6) omit from any written copies of the plan information that could expose vulnerabilities in the agency's

network or online systems; and

(7) consider whether network threat detection and response solutions, that permit anonymized security reports to be shared among participating entities in as close to real time as possible, would enhance the plan and include those solutions as part of the plan as the agency determines appropriate.

SECTION 2. Section 2054.136, Government Code, is amended to read as follows:

Sec. 2054.136. DESIGNATED INFORMATION SECURITY OFFICER. Each state agency shall designate an information security officer who:

(1) acts independently of the agency in the performance of the officer's duties under this chapter and reports to the department on information security issues and to the agency's executive-level management on other issues;

(2) has authority over information security for the entire agency;

(3) possesses the training and experience required to perform the duties required by department rules; and

(4) to the extent feasible, has information security duties as the officer's primary duties.

SECTION 3. Sections 2054.512(d) and (e), Government Code, are amended to read as follows:

(d) The cybersecurity council shall:

(1) consider the costs and benefits of establishing a computer emergency readiness team to address cyber attacks occurring in this state during routine and emergency situations;

(2) establish criteria and priorities for addressing cybersecurity threats to critical state installations;

(3) consolidate and synthesize best practices to assist state agencies in understanding and implementing cybersecurity measures, including network threat detection and response solutions, that are most beneficial to this state; and

(4) assess the knowledge, skills, and capabilities of the existing information technology and cybersecurity workforce to mitigate and respond to cyber threats and develop recommendations for addressing immediate workforce deficiencies and ensuring a long-term pool of qualified applicants.

(e) The cybersecurity council shall provide recommendations to the legislature on any legislation necessary to implement cybersecurity best practices and remediation strategies for this state, including network threat detection and response solutions.

SECTION 4. Section 2054.518(a), Government Code, is amended to read as follows:

(a) The department shall develop a plan to address cybersecurity risks and incidents in this state. The department may enter into an agreement with a national organization, including the National Cybersecurity Preparedness Consortium, to support the department's efforts in implementing the components of the plan for which the department lacks resources to address internally. The agreement may include provisions for:

(1) providing technical assistance services to support preparedness for and response to cybersecurity risks and incidents;

(2) conducting cybersecurity simulation exercises for state agencies to encourage coordination in defending against and responding to cybersecurity risks and incidents;

(3) assisting state agencies in developing cybersecurity information-sharing programs to disseminate information related to cybersecurity risks and incidents; [~~and~~]

(4) incorporating cybersecurity risk and incident prevention and response methods into existing state emergency plans, including continuity of operation plans and incident response plans; and

(5) incorporating network threat detection and response solutions into state agency cybersecurity plans, that permit anonymized security reports to be shared among participating entities in as close to real time as possible, to assist state agencies with monitoring agency networks for security threats and responding to detected security threats.

SECTION 5. This Act takes effect September 1, 2023.