By: Blanco H.B. No. 4597

A BILL TO BE ENTITLED

AN ACT

relating to cybersecurity of state agencies.

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

SECTION 1. Section 552. 139 (b), Government Code, is amended to read as follows:

(b) The following information is confidential:

(1) a computer network vulnerability report;

(2) any other assessment of the extent to which data processing operations, a computer, a computer program, network, system, or system interface, or software of a governmental body or of a contractor of a governmental body is vulnerable to unauthorized access or harm, including an assessment of the extent to which the governmental body's or contractor's electronically stored information containing sensitive or critical information is vulnerable to alteration, damage, erasure, or inappropriate use;

(3) a photocopy of other copy of an identification badge issued to an official or employee of a governmental body; [~~and~~]

(4) information directly arising from a governmental body's routine to prevent, detect, investigate, or mitigate a computer security incident, including information contained in or derived from an information security log; and

(5) information about a state agency's cybersecurity insurance coverage, including policy provisions and coverage

limits.

SECTION 2. Subchapter N-1, Chapter 2054, Government Code, is amended by adding Section 2054.5172 to read as follows:

Sec. 2054.5172. CYBER RANGE. (a) In this section, "cyber range" means a virtual environment used for interactive training in the defense against and response to cyberwarfare and other cybersecurity incidents.

(b) The department may create a cyber range for use by public sector employees with responsibility for cybersecurity to improve this state's cybersecurity capabilities.

SECTION 3. Subchapter N-1, Chapter 2054, Government Code, is amended by adding Section 2054.519, 2054.520, and 2054.521 to read as follows:

Sec. 2054.519. CYBERSECURITY RESOURCES PROGRAM FOR STATE AGENCIES. (a) The department may establish a program that provides to state agencies the use of information security officers and other cybersecurity resources to assist in managing the agencies' information security.

(b) The department shall adopt rules to implement this section.

Sec. 2054.520. CYBERSECURITY INSURANCE. (a) The State Office of Risk Management shall evaluate the feasibility of providing cybersecurity insurance policies to state agencies.

(b) The State Office of Risk Management shall develop guidance for state agencies regarding cybersecurity insurance coverage. The guidance must:

(1) be based on best practices for making

cybersecurity insurance coverage decisions; and

(2) assist a state agency in determining whether:

(A) cybersecurity insurance coverage would be beneficial to the agency; and

(B) the agency should purchase a cybersecurity insurance policy from a third party or self-insure.

(c) The department shall review and consider the guidance developed under this section in connection with the department's protection of statewide technology centers.

Sec. 2054.521. BUG BOUNTY PROGRAM. (a) The department by rule may establish a bug bounty program, using money available for that purpose from legislative appropriations, to pay bounties to persons who uncover or resolve security flaws in state websites and applications.

(b) The department may determine eligibility criteria for receiving a bounty under this section and the amount of a bounty to be paid under this section.

(c) An employee of or contractor with a state agency is not eligible to receive a bounty under this section.

(d) The payment of a bounty under this section does not affect a person 's civil or criminal liability for prohibited conduct related to a state website or application.

SECTION 4. Section 2054.136, Government Code, is amended to read as follows:

Sec. 2054.136. DESIGNATED INFORMATION SECURITY OFFICER; DUTIES. (a) In this section, "cloud computing service" has the meaning assigned by Section 2157.007.

(b) Each state agency shall designate an information security officer who:

(1) reports to the agency 's executive-level management;

(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.

(c) A state agency 's information security officer must authorize the purchase of cloud computing services before the agency may enter into a contract for those services.

SECTION 5. Section 2054.1125, Government Code, is amended by adding Subsection (c) to read as follows:

(c) Not later than the 10th business day after the date of the eradication, closure, and recovery from a breach, suspected breach, or unauthorized exposure, a state agency shall notify the department, including the chief information security officer, of the details of the event.

SECTION 6. The change in law made by this Act applies only to a contract for cloud computing services that is entered into on or after the effective date of this Act. A contract entered into before the effective date of this Act is governed by the law in effect on the date the contract was entered into, and the former law is continued in effect for that purpose.

SECTION 7. This Act takes effect September 1, 2019.