AN ACT

relating to cybersecurity for state agency information resources.

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

SECTION 1. This Act may be cited as the Texas Cybersecurity Act.

SECTION 2. Section 325.011, Government Code, is amended to read as follows:

Sec. 325.011. CRITERIA FOR REVIEW. The commission and its staff shall consider the following criteria in determining whether a public need exists for the continuation of a state agency or its advisory committees or for the performance of the functions of the agency or its advisory committees:

(1) the efficiency and effectiveness with which the agency or the advisory committee operates;

(2)(A) an identification of the mission, goals, and objectives intended for the agency or advisory committee and of the problem or need that the agency or advisory committee was intended to address; and

(B) the extent to which the mission, goals, and objectives have been achieved and the problem or need has been addressed;

(3)(A) an identification of any activities of the agency in addition to those granted by statute and of the authority for those activities; and

(B) the extent to which those activities are needed;

(4) an assessment of authority of the agency relating to fees, inspections, enforcement, and penalties;

(5) whether less restrictive or alternative methods of performing any function that the agency performs could adequately protect or provide service to the public;

(6) the extent to which the jurisdiction of the agency and the programs administered by the agency overlap or duplicate those of other agencies, the extent to which the agency coordinates with those agencies, and the extent to which the programs administered by the agency can be consolidated with the programs of other state agencies;

(7) the promptness and effectiveness with which the agency addresses complaints concerning entities or other persons affected by the agency, including an assessment of the agency's administrative hearings process;

(8) an assessment of the agency's rulemaking process and the extent to which the agency has encouraged participation by the public in making its rules and decisions and the extent to which the public participation has resulted in rules that benefit the public;

(9) the extent to which the agency has complied with:

(A) federal and state laws and applicable rules regarding equality of employment opportunity and the rights and privacy of individuals; and

(B) state law and applicable rules of any state

agency regarding purchasing guidelines and programs for historically underutilized businesses;

(10) the extent to which the agency issues and enforces rules relating to potential conflicts of interest of its employees;

(11) the extent to which the agency complies with Chapters 551 and 552 and follows records management practices that enable the agency to respond efficiently to requests for public information;

(12) the effect of federal intervention or loss of federal funds if the agency is abolished; [~~and~~]

(13) the extent to which the purpose and effectiveness of reporting requirements imposed on the agency justifies the continuation of the requirement; and

(14) an assessment of the agency's cybersecurity practices using confidential information available from the Department of Information Resources or any other appropriate state agency.

SECTION 3. Section 551.089, Government Code, is amended to read as follows:

Sec. 551.089. DELIBERATION REGARDING SECURITY DEVICES OR SECURITY AUDITS; CLOSED MEETING [~~DEPARTMENT OF INFORMATION RESOURCES~~]. This chapter does not require a governmental body [~~the governing board of the Department of Information Resources~~] to conduct an open meeting to deliberate:

(1) security assessments or deployments relating to information resources technology;

(2) network security information as described by Section 2059.055(b); or

(3) the deployment, or specific occasions for implementation, of security personnel, critical infrastructure, or security devices.

SECTION 4. Section 552.139, Government Code, is amended by adding Subsection (d) to read as follows:

(d) When posting a contract on an Internet website as required by Section 2261.253, a state agency shall redact information made confidential by this section or excepted from public disclosure by this section. Redaction under this subsection does not except information from the requirements of Section 552.021.

SECTION 5. Subchapter C, Chapter 2054, Government Code, is amended by adding Section 2054.0594 to read as follows:

Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS CENTER. (a) The department shall establish an information sharing and analysis center to provide a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies.

(b) The department shall appoint persons from appropriate state agencies to serve as representatives to the information sharing and analysis center.

(c) The department, using funds other than funds appropriated to the department in a general appropriations act, shall provide administrative support to the information sharing and analysis center.

SECTION 6. Section 2054.076, Government Code, is amended by adding Subsection (b-1) to read as follows:

(b-1) The department shall provide mandatory guidelines to state agencies regarding the continuing education requirements for cybersecurity training that must be completed by all information resources employees of the agencies. The department shall consult with the Information Technology Council for Higher Education on applying the guidelines to institutions of higher education.

SECTION 7. Sections 2054.077(b) and (e), Government Code, are amended to read as follows:

(b) The information resources manager of a state agency shall [~~may~~] prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than October 15 of each even-numbered year, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use.

(e) Separate from the executive summary described by Subsection (b), a state agency [~~whose information resources manager has prepared or has had prepared a vulnerability report~~] shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise

the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request.

SECTION 8. Section 2054.1125(b), Government Code, is amended to read as follows:

(b) A state agency that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

(1) comply[~~, in the event of a breach of system security,~~] with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state; and

(2) not later than 48 hours after the discovery of the breach, suspected breach, or unauthorized exposure, notify:

(A) the department, including the chief information security officer and the state cybersecurity coordinator; or

(B) if the breach, suspected breach, or unauthorized exposure involves election data, the secretary of state.

SECTION 9. Section 2054.512, Government Code, is amended to read as follows:

Sec. 2054.512. CYBERSECURITY [~~PRIVATE INDUSTRY-GOVERNMENT~~] COUNCIL. (a) The state cybersecurity coordinator shall [~~may~~] establish and lead a cybersecurity council that includes public and private sector leaders and cybersecurity practitioners to collaborate on matters of cybersecurity concerning this state.

(b) The cybersecurity council must include:

(1) one member who is an employee of the office of the governor;

(2) one member of the senate appointed by the lieutenant governor;

(3) one member of the house of representatives appointed by the speaker of the house of representatives; and

(4) additional members appointed by the state cybersecurity coordinator, including representatives of institutions of higher education and private sector leaders.

(c) In appointing representatives from institutions of higher education to the cybersecurity council, the state cybersecurity coordinator shall consider appointing members of the Information Technology Council for Higher Education.

(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 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.

SECTION 10. Section 2054.133, Government Code, is amended by adding Subsection (e) to read as follows:

(e) Each state agency shall include in the agency's information security plan a written acknowledgment that the executive director or other head of the agency, the chief financial officer, and each executive manager as designated by the state agency have been made aware of the risks revealed during the preparation of the agency's information security plan.

SECTION 11. Subchapter N-1, Chapter 2054, Government Code, is amended by adding Sections 2054.515, 2054.516, 2054.517, and 2054.518 to read as follows:

Sec. 2054.515. AGENCY INFORMATION SECURITY ASSESSMENT AND REPORT. (a) At least once every two years, each state agency shall conduct an information security assessment of the agency's information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities.

(b) Not later than December 1 of the year in which a state agency conducts the assessment under Subsection (a), the agency shall report the results of the assessment to the department, the governor, the lieutenant governor, and the speaker of the house of representatives.

(c) The department by rule may establish the requirements for the information security assessment and report required by this section.

Sec. 2054.516. DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS. Each state agency, other than an institution of higher education subject to Section 2054.517, implementing an Internet website or mobile application that processes any sensitive personal information or confidential information must:

(1) submit a biennial data security plan to the department not later than October 15 of each even-numbered year to establish planned beta testing for the website or application; and

(2) subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.

Sec. 2054.517. DATA SECURITY PROCEDURES FOR ONLINE AND MOBILE APPLICATIONS OF INSTITUTIONS OF HIGHER EDUCATION. (a) Each institution of higher education, as defined by Section 61.003, Education Code, shall adopt and implement a policy for Internet website and mobile application security procedures that complies with this section.

(b) Before deploying an Internet website or mobile application that processes confidential information for an

institution of higher education, the developer of the website or application for the institution must submit to the institution's information security officer the information required under policies adopted by the institution to protect the privacy of individuals by preserving the confidentiality of information processed by the website or application. At a minimum, the institution's policies must require the developer to submit information describing:

(1) the architecture of the website or application;

(2) the authentication mechanism for the website or application; and

(3) the administrator level access to data included in the website or application.

(c) Before deploying an Internet website or mobile application described by Subsection (b), an institution of higher education must subject the website or application to a vulnerability and penetration test conducted internally or by an independent third party.

(d) Each institution of higher education shall submit to the department the policies adopted as required by Subsection (b). The department shall review the policies and make recommendations for appropriate changes.

Sec. 2054.518. CYBERSECURITY RISKS AND INCIDENTS. (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 fee reimbursement for appropriate industry-recognized certification examinations for and training to state agencies preparing for and responding to cybersecurity risks and incidents;

(2) developing and maintaining a cybersecurity risks and incidents curriculum using existing programs and models for training state agencies;

(3) delivering to state agency personnel with access to state agency networks routine training related to appropriately protecting and maintaining information technology systems and devices, implementing cybersecurity best practices, and mitigating cybersecurity risks and vulnerabilities;

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

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

(6) assisting state agencies in developing cybersecurity information-sharing programs to disseminate information related to cybersecurity risks and incidents; and

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

response plans.

(b) In implementing the provisions of the agreement prescribed by Subsection (a), the department shall seek to prevent unnecessary duplication of existing programs or efforts of the department or another state agency.

(c) In selecting an organization under Subsection (a), the department shall consider the organization's previous experience in conducting cybersecurity training and exercises for state agencies and political subdivisions.

(d) The department shall consult with institutions of higher education in this state when appropriate based on an institution's expertise in addressing specific cybersecurity risks and incidents.

SECTION 12. Section 2054.575(a), Government Code, is amended to read as follows:

(a) A state agency shall, with available funds, identify information security issues and develop a plan to prioritize the remediation and mitigation of those issues. The agency shall include in the plan:

(1) procedures for reducing the agency's level of exposure with regard to information that alone or in conjunction with other information identifies an individual maintained on a legacy system of the agency;

(2) the best value approach for modernizing, replacing, renewing, or disposing of a legacy system that maintains information critical to the agency's responsibilities;

(3) analysis of the percentage of state agency

personnel in information technology, cybersecurity, or other cyber-related positions who currently hold the appropriate industry-recognized certifications as identified by the National Initiative for Cybersecurity Education;

(4) the level of preparedness of state agency cyber personnel and potential personnel who do not hold the appropriate industry-recognized certifications to successfully complete the industry-recognized certification examinations; and

(5) a strategy for mitigating any workforce-related discrepancy in information technology, cybersecurity, or other cyber-related positions with the appropriate training and industry-recognized certifications.

SECTION 13. Section 2059.055(b), Government Code, is amended to read as follows:

(b) Network security information is confidential under this section if the information is:

(1) related to passwords, personal identification numbers, access codes, encryption, or other components of the security system of a governmental entity [~~state agency~~];

(2) collected, assembled, or maintained by or for a governmental entity to prevent, detect, or investigate criminal activity; or

(3) related to an assessment, made by or for a governmental entity or maintained by a governmental entity, of the vulnerability of a network to criminal activity.

SECTION 14. Chapter 276, Election Code, is amended by adding Section 276.011 to read as follows:

Sec. 276.011. ELECTION CYBER ATTACK STUDY. (a) Not later than December 1, 2018, the secretary of state shall:

(1) conduct a study regarding cyber attacks on election infrastructure;

(2) prepare a public summary report on the study's findings that does not contain any information the release of which may compromise any election;

(3) prepare a confidential report on specific findings and vulnerabilities that is exempt from disclosure under Chapter 552, Government Code; and

(4) submit to the standing committees of the legislature with jurisdiction over election procedures a copy of the report required under Subdivision (2) and a general compilation of the report required under Subdivision (3) that does not contain any information the release of which may compromise any election.

(b) The study must include:

(1) an investigation of vulnerabilities and risks for a cyber attack against a county's voting system machines or the list of registered voters;

(2) information on any attempted cyber attack on a county's voting system machines or the list of registered voters; and

(3) recommendations for protecting a county's voting system machines and list of registered voters from a cyber attack.

(c) The secretary of state, using existing resources, may contract with a qualified vendor to conduct the study required by this section.

(d) This section expires January 1, 2019.

SECTION 15. (a) The lieutenant governor shall establish a Senate Select Committee on Cybersecurity and the speaker of the house of representatives shall establish a House Select Committee on Cybersecurity to, jointly or separately, study:

(1) cybersecurity in this state;

(2) the information security plans of each state agency; and

(3) the risks and vulnerabilities of state agency cybersecurity.

(b) Not later than November 30, 2017:

(1) the lieutenant governor shall appoint five senators to the Senate Select Committee on Cybersecurity, one of whom shall be designated as chair; and

(2) the speaker of the house of representatives shall appoint five state representatives to the House Select Committee on Cybersecurity, one of whom shall be designated as chair.

(c) The committees established under this section shall convene separately at the call of the chair of the respective committees, or jointly at the call of both chairs. In joint meetings, the chairs of each committee shall act as joint chairs.

(d) Following consideration of the issues listed in Subsection (a) of this section, the committees established under this section shall jointly adopt recommendations on state cybersecurity and report in writing to the legislature any findings and adopted recommendations not later than January 13, 2019.

(e) This section expires September 1, 2019.

SECTION 16. (a) In this section, "state agency" means a board, commission, office, department, council, authority, or other agency in the executive or judicial branch of state government that is created by the constitution or a statute of this state. The term does not include a university system or institution of higher education as those terms are defined by Section 61.003, Education Code.

(b) The Department of Information Resources, in consultation with the Texas State Library and Archives Commission, shall conduct a study on state agency digital data storage and records management practices and the associated costs to this state.

(c) The study required under this section must examine:

(1) the current digital data storage practices of state agencies in this state;

(2) the costs associated with those digital data storage practices;

(3) the digital records management and data classification policies of state agencies and whether the state agencies are consistently complying with the established policies;

(4) whether the state agencies are storing digital data that exceeds established retention requirements and the cost of that unnecessary storage;

(5) the adequacy of storage systems used by state agencies to securely maintain confidential digital records;

(6) possible solutions and improvements recommended by the state agencies for reducing state costs and increasing

security for digital data storage and records management; and

(7) the security level and possible benefits of and the cost savings from using cloud computing services for agency data storage, data classification, and records management.

(d) Each state agency shall participate in the study required by this section and provide appropriate assistance and information to the Department of Information Resources and the Texas State Library and Archives Commission.

(e) Not later than December 1, 2018, the Department of Information Resources shall issue a report on the study required under this section and recommendations for reducing state costs and for improving efficiency in digital data storage and records management to the lieutenant governor, the speaker of the house of representatives, and the appropriate standing committees of the house of representatives and the senate.

(f) This section expires September 1, 2019.

SECTION 17. The changes in law made by this Act do not apply to the Electric Reliability Council of Texas.

SECTION 18. This Act takes effect September 1, 2017.

President of the Senate

Speaker of the House

I certify that H.B. No. 8 was passed by the House on April 25, 2017, by the following vote: Yeas 145, Nays 0, 2 present, not voting; and that the House concurred in Senate amendments to H.B. No. 8 on May 27, 2017, by the following vote: Yeas 139, Nays 7, 2 present, not voting.

Chief Clerk of the House

I certify that H.B. No. 8 was passed by the Senate, with amendments, on May 24, 2017, by the following vote: Yeas 31, Nays 0.

Secretary of the Senate

APPROVED: _____

Date

_____

Governor