

SENATE AMENDMENTS

2nd Printing

By: Capriglione, Elkins, Parker, Dale, Dean,
et al.

H.B. No. 8

A BILL TO BE ENTITLED

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

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

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

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

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

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

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

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

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

27 (B) state law and applicable rules of any state

1 agency regarding purchasing guidelines and programs for
2 historically underutilized businesses;

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

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

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

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

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

18 SECTION 3. Subchapter B, Chapter 421, Government Code, is
19 amended by adding Section 421.027 to read as follows:

20 Sec. 421.027. CYBER INCIDENT STUDY AND RESPONSE PLAN. (a)
21 In this section:

22 (1) "Cyber incident" means an event occurring on or
23 conducted through a computer network that actually or imminently
24 jeopardizes the integrity, confidentiality, or availability of
25 computers, information or communications systems or networks,
26 physical or virtual infrastructure controlled by computers or
27 information systems, or information on the computers or systems.

1 The term includes a vulnerability in implementation or in an
2 information system, system security procedure, or internal control
3 that could be exploited by a threat source.

4 (2) "Significant cyber incident" means a cyber
5 incident, or a group of related cyber incidents, likely to result in
6 demonstrable harm to state security interests, foreign relations,
7 or the economy of this state or to the public confidence, civil
8 liberties, or public health and safety of the residents of this
9 state.

10 (b) The council, in cooperation with the Department of
11 Information Resources, shall:

12 (1) conduct a study regarding cyber incidents and
13 significant cyber incidents affecting state agencies and critical
14 infrastructure that is owned, operated, or controlled by agencies;
15 and

16 (2) develop a comprehensive state response plan to
17 provide a format for each state agency to develop an
18 agency-specific response plan and to implement the plan into the
19 agency's information security plan required under Section 2054.133
20 to be implemented by the agency in the event of a cyber incident or
21 significant cyber incident affecting the agency or critical
22 infrastructure that is owned, operated, or controlled by the
23 agency.

24 (c) Not later than September 1, 2018, the council shall
25 deliver the response plan and a report on the findings of the study
26 to:

27 (1) the public safety director of the Department of

1 Public Safety;

2 (2) the governor;

3 (3) the lieutenant governor;

4 (4) the speaker of the house of representatives;

5 (5) the chair of the committee of the senate having
6 primary jurisdiction over homeland security matters; and

7 (6) the chair of the committee of the house of
8 representatives having primary jurisdiction over homeland security
9 matters.

10 (d) The response plan required by Subsection (b) and the
11 report required by Subsection (c) are not public information for
12 purposes of Chapter 552.

13 (e) This section expires December 1, 2018.

14 SECTION 4. Section 551.089, Government Code, is amended to
15 read as follows:

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

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

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

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

SECTION 5. 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 6. The heading to Section 656.047, Government Code, is amended to read as follows:

Sec. 656.047. PAYMENT OF PROGRAM AND CERTIFICATION EXAMINATION EXPENSES.

SECTION 7. Section 656.047, Government Code, is amended by adding Subsection (a-1) to read as follows:

(a-1) A state agency may spend public funds as appropriate to reimburse a state agency employee or administrator who serves in an information technology, cybersecurity, or other cyber-related position for fees associated with industry-recognized certification examinations.

SECTION 8. 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

1 state agencies to serve as representatives to the information
2 sharing and analysis center.

3 (c) The department, using existing resources, shall provide
4 administrative support to the information sharing and analysis
5 center.

6 SECTION 9. Section 2054.076, Government Code, is amended by
7 adding Subsection (b-1) to read as follows:

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

15 SECTION 10. Sections 2054.077(b) and (e), Government Code,
16 are amended to read as follows:

17 (b) The information resources manager of a state agency
18 shall ~~[may]~~ prepare or have prepared a report, including an
19 executive summary of the findings of the report, assessing the
20 extent to which a computer, a computer program, a computer network,
21 a computer system, a printer, an interface to a computer system,
22 including mobile and peripheral devices, computer software, or data
23 processing of the agency or of a contractor of the agency is
24 vulnerable to unauthorized access or harm, including the extent to
25 which the agency's or contractor's electronically stored
26 information is vulnerable to alteration, damage, erasure, or
27 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 11. 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

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

4 SECTION 12. Section 2054.133, Government Code, is amended
5 by adding Subsections (b-1), (b-2), (b-3), and (b-4) to read as
6 follows:

7 (b-1) The executive head and chief information security
8 officer of each state agency shall annually review and approve in
9 writing the agency's information security plan and strategies for
10 addressing the agency's information resources systems that are at
11 highest risk for security breaches. The plan at a minimum must
12 include solutions that isolate and segment sensitive information
13 and maintain architecturally sound and secured separation among
14 networks. If a state agency does not have a chief information
15 security officer, the highest ranking information security
16 employee for the agency shall review and approve the plan and
17 strategies. The executive head retains full responsibility for the
18 agency's information security and any risks to that security.

19 (b-2) Before submitting to the Legislative Budget Board a
20 legislative appropriation request for a state fiscal biennium, a
21 state agency must file with the board the written approval required
22 under Subsection (b-1) for each year of the current state fiscal
23 biennium.

24 (b-3) Each state agency shall include in the agency's
25 information security plan the actions the agency is taking to
26 incorporate into the plan the core functions of "identify, protect,
27 detect, respond, and recover" as recommended in the "Framework for

Improving Critical Infrastructure Cybersecurity" of the United States Department of Commerce National Institute of Standards and Technology. The agency shall, at a minimum, identify any information the agency requires individuals to provide to the agency or the agency retains that is not necessary for the agency's operations. The agency may incorporate the core functions over a period of years.

(b-4) A state agency's information security plan must include appropriate privacy and security standards that, at a minimum, require a vendor who offers cloud computing services or other software, applications, online services, or information technology solutions to any state agency to contractually warrant that data provided by the state to the vendor will be maintained in compliance with all applicable state and federal laws and rules.

SECTION 13. 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 appointed by 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

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

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

8 (d) The cybersecurity council shall provide recommendations
9 to the legislature on any legislation necessary to implement
10 cybersecurity best practices and remediation strategies for this
11 state.

12 SECTION 14. Subchapter N-1, Chapter 2054, Government Code,
13 is amended by adding Sections 2054.515, 2054.516, 2054.517,
14 2054.518, and 2054.519 to read as follows:

15 Sec. 2054.515. INDEPENDENT RISK ASSESSMENT. (a) At least
16 once every five years, in accordance with department rules, each
17 state agency shall:

18 (1) contract with an independent third party selected
19 from a list provided by the department to conduct an independent
20 risk assessment of the agency's exposure to security risks in the
21 agency's information resources systems and to conduct tests to
22 practice securing systems and notifying all affected parties in the
23 event of a data breach; and

24 (2) submit the results of the independent risk
25 assessment to the department.

26 (b) The department annually shall compile the results of the
27 independent risk assessments conducted in the preceding year and

1 prepare:

2 (1) a public report on the general security issues
3 covered by the assessments that does not contain any information
4 the release of which may compromise any state agency's information
5 resources system; and

6 (2) a confidential report on specific risks and
7 vulnerabilities that is exempt from disclosure under Chapter 552.

8 (c) The department annually shall submit to the legislature
9 a comprehensive report on the results of the independent risk
10 assessments conducted under Subsection (a) during the preceding
11 year that includes the report prepared under Subsection (b)(1) and
12 that identifies systematic or pervasive security risk
13 vulnerabilities across state agencies and recommendations for
14 addressing the vulnerabilities but does not contain any information
15 the release of which may compromise any state agency's information
16 resources system.

17 Sec. 2054.516. DATA SECURITY PLAN FOR ONLINE AND MOBILE
18 APPLICATIONS. (a) Each state agency, other than an institution of
19 higher education subject to Section 2054.517, implementing an
20 Internet website or mobile application that processes any
21 personally identifiable or confidential information must:

22 (1) submit a data security plan to the department
23 during development and as early as feasible in the testing of the
24 website or application and submit any modification to the plan made
25 during development; and

26 (2) before deploying the website or application:

27 (A) subject the website or application to a

vulnerability and penetration test conducted by an independent third party; and

(B) address any high priority vulnerability identified under Paragraph (A).

(b) The data security plan required under Subsection (a)(1) must include:

(1) data flow diagrams to show the location of information in use, in transit, and not in use;

(2) data storage locations;

(3) data interaction with online or mobile devices;

(4) security of data transfer;

(5) security measures for the online or mobile application;

(6) a description of any action taken by the agency to remediate any vulnerability identified by an independent third party under Subsection (a)(2); and

(7) appropriate privacy and security standards that, at a minimum, require a vendor who offers cloud computing services or other software, applications, online services, or information technology solutions to any state agency to demonstrate that data provided by the state to the vendor will be maintained in compliance with all applicable state and federal laws and rules.

(c) Unless a state agency has previously submitted a comprehensive security plan approved by the department and has sufficient personnel and technology to review plans internally, the department shall review each data security plan submitted under Subsection (a) and make any recommendations for changes to the plan

1 to the state agency as soon as practicable after the department
2 reviews the plan.

3 (d) A data security plan submitted under Subsection (a) and
4 any recommendation for changes made under Subsection (c) are not
5 public information for purposes of Chapter 552.

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

12 (b) Before deploying an Internet website or mobile
13 application that processes confidential information for an
14 institution of higher education, the developer of the website or
15 application for the institution must submit to the institution's
16 information security officer the information required under
17 policies adopted by the institution to protect the privacy of
18 individuals by preserving the confidentiality of information
19 processed by the website or application. At a minimum, the
20 institution's policies must require the developer to submit
21 information describing:

- 22 (1) the architecture of the website or application;
23 (2) the authentication mechanism for the website or
24 application; and
25 (3) the administrator level access to data included in
26 the website or application.

27 (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. VENDOR RESPONSIBILITY FOR CYBERSECURITY. A vendor that contracts with this state to provide information resources technology for a state agency at a cost to the agency of \$1 million or more is responsible for addressing known cybersecurity risks associated with the technology and is responsible for any cost associated with addressing the identified cybersecurity risks. For a major information resources project, the vendor shall provide to state agency contracting personnel:

(1) written acknowledgment of any known cybersecurity risks associated with the technology identified in the vulnerability and penetration test conducted under Section 2054.516 or Section 2054.517;

(2) proof that any individual servicing the contract holds the appropriate industry-recognized certifications as identified by the National Initiative for Cybersecurity Education;

(3) a strategy for mitigating any technology or personnel-related cybersecurity risk identified in the vulnerability and penetration test conducted under Section 2054.516 or Section 2054.517; and

1 (4) an initial summary of any costs associated with
2 addressing or remediating the identified technology or
3 personnel-related cybersecurity risks as identified in
4 collaboration with this state following a risk assessment.

5 Sec. 2054.519. CYBERSECURITY RISKS AND INCIDENTS. (a) The
6 department shall develop a plan to address cybersecurity risks and
7 incidents in this state. The department may enter into an agreement
8 with a national organization, including the National Cybersecurity
9 Preparedness Consortium, to support the department's efforts in
10 implementing the components of the plan for which the department
11 lacks resources to address internally. The agreement may include
12 provisions for:

13 (1) providing fee reimbursement for appropriate
14 industry-recognized certification examinations for and training to
15 state and local officials and first responders preparing for and
16 responding to cybersecurity risks and incidents;

17 (2) developing and maintaining a cybersecurity risks
18 and incidents curriculum using existing programs and models for
19 training state and local officials and first responders;

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

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

1 (5) conducting cybersecurity training and simulation
2 exercises for state agencies, political subdivisions, and private
3 entities to encourage coordination in defending against and
4 responding to cybersecurity risks and incidents;

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

9 (7) incorporating cybersecurity risk and incident
10 prevention and response methods into existing state and local
11 emergency plans, including continuity of operation plans and
12 incident response plans.

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

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

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

25 SECTION 15. Section 2054.575(a), Government Code, is
26 amended to read as follows:

27 (a) A state agency shall, with available funds, identify

1 information security issues and develop a plan to prioritize the
2 remediation and mitigation of those issues. The agency shall
3 include in the plan:

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

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

11 (3) analysis of the percentage of state agency
12 personnel in information technology, cybersecurity, or other
13 cyber-related positions who currently hold the appropriate
14 industry-recognized certifications as identified by the National
15 Initiative for Cybersecurity Education;

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

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

24 SECTION 16. Section 2059.055(b), Government Code, is
25 amended to read as follows:

26 (b) Network security information is confidential under this
27 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 17. Subtitle B, Title 10, Government Code, is amended by adding Chapter 2061 to read as follows:

CHAPTER 2061. INDIVIDUAL-IDENTIFYING INFORMATION

Sec. 2061.001. DEFINITIONS. In this chapter:

(1) "Cybersecurity risk" means a material threat of attack, damage, or unauthorized access to the networks, computers, software, or data storage of a state agency.

(2) "State agency" means a department, commission, board, office, council, authority, or other agency in the executive, legislative, or judicial branch of state government, including a university system or institution of higher education, as defined by Section 61.003, Education Code, that is created by the constitution or a statute of this state.

Sec. 2061.002. DESTRUCTION AUTHORIZED. (a) A state agency shall destroy or arrange for the destruction of information that presents a cybersecurity risk and alone or in conjunction with other information identifies an individual in connection with the agency's networks, computers, software, or data storage if the

1 agency is otherwise prohibited by law from retaining the
2 information for a period of years.

3 (b) A state agency shall destroy or arrange for the
4 destruction of information described by Subsection (a) in
5 accordance with standards for destruction of data prescribed in the
6 National Security Program Operating Manual, 1995 edition.

7 (c) This section does not apply to a record involving
8 criminal activity or a criminal investigation retained for law
9 enforcement purposes.

10 (d) A state agency may not destroy or arrange for the
11 destruction of any election data before the third anniversary of
12 the date the election to which the data pertains is held.

13 (e) A state agency may not under any circumstance sell:

14 (1) a person's precise geographic location
15 information;

16 (2) a person's Internet browsing history;

17 (3) a person's application usage history; or

18 (4) the functional equivalent of the information
19 described in Subdivisions (1)-(3).

20 (f) Not later than September 1, 2019, each state agency
21 shall develop the systems and policies necessary to comply with
22 this section. This subsection expires September 1, 2020.

23 SECTION 18. Section 2157.007, Government Code, is amended
24 by adding Subsection (e) to read as follows:

25 (e) The department shall periodically review guidelines on
26 state agency information that may be stored by a cloud computing or
27 other storage service and the cloud computing or other storage

services available to state agencies for that storage to ensure that an agency purchasing a major information resources project under Section 2054.118 selects the most affordable, secure, and efficient cloud computing or other storage service available to the agency. The guidelines must include appropriate privacy and security standards that, at a minimum, require a vendor who offers cloud computing or other storage services or other software, applications, online services, or information technology solutions to any state agency to demonstrate that data provided by the state to the vendor will be maintained in compliance with all applicable state and federal laws and rules.

SECTION 19. 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 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 to the standing

committees of the legislature with jurisdiction over election procedures.

(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 20. (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

1 whom shall be designated as chair; and

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

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

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

14 (e) This section expires September 1, 2019.

15 SECTION 21. (a) In this section, "state agency" means a
16 board, commission, office, department, council, authority, or
17 other agency in the executive or judicial branch of state
18 government that is created by the constitution or a statute of this
19 state. The term does not include a university system or institution
20 of higher education as those terms are defined by Section 61.003,
21 Education Code.

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

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

27 (1) the current digital data storage practices of

1 state agencies in this state;

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

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

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

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

12 (6) possible solutions and improvements recommended
13 by the state agencies for reducing state costs and increasing
14 security for digital data storage and records management; and

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

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

22 (e) Not later than December 1, 2018, the Department of
23 Information Resources and the Texas State Library and Archives
24 Commission shall issue a report on the study required under this
25 section and recommendations for reducing state costs and for
26 improving efficiency in digital data storage and records management
27 to the lieutenant governor, the speaker of the house of

1 representatives, and the appropriate standing committees of the
2 house of representatives and the senate.

3 (f) This section expires September 1, 2019.

4 SECTION 22. The changes in law made by this Act do not apply
5 to the Electric Reliability Council of Texas.

6 SECTION 23. This Act takes effect September 1, 2017.

ADOPTED

MAY 24 2017

Leroy Spaw
Secretary of the Senate

By: Nelson

H.B. No. 8

Substitute the following for ____B. No. ____:

By: Brandon Coughlin

C.S. ____B. No. ____

A BILL TO BE ENTITLED

1 AN ACT

2 relating to cybersecurity for state agency information resources.

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

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

6 SECTION 2. Section 551.089, Government Code, is amended to
7 read as follows:

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

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

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

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

20 SECTION 3. Section 552.139, Government Code, is amended by
21 adding Subsection (d) to read as follows:

22 (d) When posting a contract on an Internet website as
23 required by Section 2261.253, a state agency shall redact
24 information made confidential by this section or excepted from

1 public disclosure by this section. Redaction under this subsection
2 does not except information from the requirements of Section
3 552.021.

4 SECTION 4. Subchapter C, Chapter 2054, Government Code, is
5 amended by adding Section 2054.0594 to read as follows:

6 Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS CENTER.

7 (a) The department shall establish an information sharing and
8 analysis center to provide a forum for state agencies to share
9 information regarding cybersecurity threats, best practices, and
10 remediation strategies.

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

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

18 SECTION 5. Sections 2054.077(b) and (e), Government Code,
19 are amended to read as follows:

20 (b) The information resources manager of a state agency may
21 prepare or have prepared a report, including an executive summary
22 of the findings of the report, assessing the extent to which a
23 computer, a computer program, a computer network, a computer
24 system, a printer, an interface to a computer system, including
25 mobile and peripheral devices, computer software, or data
26 processing of the agency or of a contractor of the agency is
27 vulnerable to unauthorized access or harm, including the extent to

1 which the agency's or contractor's electronically stored
2 information is vulnerable to alteration, damage, erasure, or
3 inappropriate use.

4 (e) Separate from the executive summary described by
5 Subsection (b), a state agency [~~whose information resources manager~~
6 ~~has prepared or has had prepared a vulnerability report~~] shall
7 prepare a summary of the agency's vulnerability report that does
8 not contain any information the release of which might compromise
9 the security of the state agency's or state agency contractor's
10 computers, computer programs, computer networks, computer systems,
11 printers, interfaces to computer systems, including mobile and
12 peripheral devices, computer software, data processing, or
13 electronically stored information. The summary is available to
14 the public on request.

15 SECTION 6. Section 2054.1125(b), Government Code, is
16 amended to read as follows:

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

22 (1) comply[~~, in the event of a breach of system~~
23 ~~security,~~] with the notification requirements of Section 521.053,

24 Business & Commerce Code, to the same extent as a person who
25 conducts business in this state; and

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

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

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

7 SECTION 7. Section 2054.133, Government Code, is amended by
8 adding Subsections (b-1), (b-2), and (b-3) to read as follows:

9 (b-1) The executive head and information security officer
10 of each state agency shall annually review and approve in writing
11 the agency's information security plan and strategies for
12 addressing the agency's information resources systems that are at
13 highest risk for security breaches. The plan at a minimum must
14 include solutions that isolate and segment sensitive information
15 and maintain architecturally sound and secured separation among
16 networks. If a state agency does not have an information security
17 officer, the highest ranking information security employee for the
18 agency shall review and approve the plan and strategies. The
19 executive head retains full responsibility for the agency's
20 information security and any risks to that security.

21 (b-2) Each state agency shall include in the agency's
22 information security plan the actions the agency is taking to
23 incorporate into the plan the core functions of "identify, protect,
24 detect, respond, and recover" as recommended in the "Framework for
25 Improving Critical Infrastructure Cybersecurity" of the United
26 States Department of Commerce National Institute of Standards and
27 Technology. The agency shall, at a minimum, identify any

1 information the agency requires individuals to provide to the
2 agency or the agency retains that is not necessary for the agency's
3 operations. The agency may incorporate the core functions over a
4 period of years.

5 (b-3) A state agency's information security plan must
6 include appropriate privacy and security standards that, at a
7 minimum, require a vendor who offers cloud computing services or
8 other software, applications, online services, or information
9 technology solutions to any state agency to contractually warrant
10 that data provided by the state to the vendor will be maintained in
11 compliance with all applicable state and federal laws and rules as
12 specified in the applicable scope of work, request for proposal, or
13 other document requirements.

14 SECTION 8. Section 2054.512, Government Code, is amended to
15 read as follows:

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

21 (b) The cybersecurity council must include:

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

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

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

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

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

8 (d) The cybersecurity council shall provide recommendations
9 to the legislature on any legislation necessary to implement
10 cybersecurity best practices and remediation strategies for this
11 state.

12 SECTION 9. Subchapter N-1, Chapter 2054, Government Code,
13 is amended by adding Section 2054.515 to read as follows:

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

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

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

1 SECTION 10. Section 2054.575(a), Government Code, is
2 amended to read as follows:

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

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

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

14 (3) an analysis of the percentage of state agency
15 personnel in information technology, cybersecurity, or other
16 cyber-related positions who currently hold the appropriate
17 industry-recognized certifications as identified by the National
18 Initiative for Cybersecurity Education;

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

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

27 SECTION 11. Section 2059.055(b), Government Code, is

1 amended to read as follows:

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

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

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

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

13 SECTION 12. Subtitle B, Title 10, Government Code, is
14 amended by adding Chapter 2061 to read as follows:

15 CHAPTER 2061. INDIVIDUAL-IDENTIFYING INFORMATION

16 Sec. 2061.001. DEFINITIONS. In this chapter:

17 (1) "Cybersecurity risk" means a material threat of
18 attack, damage, or unauthorized access to the networks, computers,
19 software, or data storage of a state agency.

20 (2) "State agency" means a department, commission,
21 board, office, council, authority, or other agency in the
22 executive, legislative, or judicial branch of state government,
23 including a university system or institution of higher education,
24 as defined by Section 61.003, Education Code, that is created by the
25 constitution or a statute of this state.

26 Sec. 2061.002. DESTRUCTION AUTHORIZED. (a) A state agency
27 shall destroy or arrange for the destruction of information that

1 presents a cybersecurity risk and alone or in conjunction with
2 other information identifies an individual in connection with the
3 agency's networks, computers, software, or data storage if the
4 agency is otherwise prohibited by law from retaining the
5 information for a period of years.

6 (b) This section does not apply to a record involving
7 criminal activity or a criminal investigation retained for law
8 enforcement purposes.

9 (c) A state agency may not destroy or arrange for the
10 destruction of any election data before the third anniversary of
11 the date the election to which the data pertains is held.

12 (d) A state agency may not under any circumstance sell:

- 13 (1) a person's Internet browsing history;
14 (2) a person's application usage history; or
15 (3) the functional equivalent of the information
16 described in Subdivisions (1) and (2).

17 SECTION 13. Chapter 276, Election Code, is amended by
18 adding Section 276.011 to read as follows:

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

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

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

26 (3) prepare a confidential report on specific findings
27 and vulnerabilities that is exempt from disclosure under Chapter

1 552, Government Code; and

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

7 (b) The study must include:

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

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

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

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

19 (d) This section expires January 1, 2019.

20 SECTION 14. (a) The lieutenant governor shall establish a
21 Senate Select Committee on Cybersecurity and the speaker of the
22 house of representatives shall establish a House Select Committee
23 on Cybersecurity to, jointly or separately, study:

24 (1) cybersecurity in this state;

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

27 (3) the risks and vulnerabilities of state agency

1 cybersecurity.

2 (b) Not later than November 30, 2017:

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

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

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

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

18 (e) This section expires September 1, 2019.

19 SECTION 15. (a) In this section, "state agency" means a
20 board, commission, office, department, council, authority, or
21 other agency in the executive or judicial branch of state
22 government that is created by the constitution or a statute of this
23 state. The term does not include a university system or institution
24 of higher education as those terms are defined by Section 61.003,
25 Education Code.

26 (b) The Department of Information Resources, in
27 consultation with the Texas State Library and Archives Commission,

1 shall conduct a study on state agency digital data storage and
2 records management practices and the associated costs to this
3 state.

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

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

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

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

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

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

17 (6) possible solutions and improvements recommended
18 by the state agencies for reducing state costs and increasing
19 security for digital data storage and records management; and

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

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

27 (e) Not later than December 1, 2018, the Department of

1 Information Resources shall issue a report on the study required
2 under this section and recommendations for reducing state costs and
3 for improving efficiency in digital data storage and records
4 management to the lieutenant governor, the speaker of the house of
5 representatives, and the appropriate standing committees of the
6 house of representatives and the senate.

7 (f) This section expires September 1, 2019.

8 SECTION 16. The changes in law made by this Act do not apply
9 to the Electric Reliability Council of Texas.

10 SECTION 17. This Act takes effect September 1, 2017.

ADOPTED

MAY 24 2017

Letay Davis BY: Jane Nelson
Secretary of the Senate

FLOOR AMENDMENT NO. 1

1 Amend C.S.H.B. No. 8 (senate committee printing) by
2 striking all below the enacting clause and substituting the
3 following:

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

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

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

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

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

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

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

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

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

29 (5) whether less restrictive or alternative methods

1 of performing any function that the agency performs could
2 adequately protect or provide service to the public;

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

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

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

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

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

22 (B) state law and applicable rules of any state
23 agency regarding purchasing guidelines and programs for
24 historically underutilized businesses;

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

28 (11) the extent to which the agency complies with
29 Chapters 551 and 552 and follows records management practices
30 that enable the agency to respond efficiently to requests for
31 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.

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

3 Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS CENTER.

4 (a) The department shall establish an information sharing and
5 analysis center to provide a forum for state agencies to share
6 information regarding cybersecurity threats, best practices, and
7 remediation strategies.

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

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

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

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

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

26 (b) The information resources manager of a state agency
27 shall ~~may~~ prepare or have prepared a report, including an
28 executive summary of the findings of the biennial report, not
29 later than October 15 of each even-numbered year, assessing the
30 extent to which a computer, a computer program, a computer
31 network, a computer system, a printer, an interface to a

1 computer system, including mobile and peripheral devices,
2 computer software, or data processing of the agency or of a
3 contractor of the agency is vulnerable to unauthorized access or
4 harm, including the extent to which the agency's or contractor's
5 electronically stored information is vulnerable to alteration,
6 damage, erasure, or inappropriate use.

7 (e) Separate from the executive summary described by
8 Subsection (b), a state agency [~~whose information resources~~
9 ~~manager has prepared or has had prepared a vulnerability report~~]
10 shall prepare a summary of the agency's vulnerability report
11 that does not contain any information the release of which might
12 compromise the security of the state agency's or state agency
13 contractor's computers, computer programs, computer networks,
14 computer systems, printers, interfaces to computer systems,
15 including mobile and peripheral devices, computer software, data
16 processing, or electronically stored information. The summary
17 is available to the public on request.

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

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

26 (1) comply[~~, in the event of a breach of system~~
27 ~~security,~~ with the notification requirements of Section
28 521.053, Business & Commerce Code, to the same extent as a
29 person who conducts business in this state; and

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

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

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

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

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

14 (b) The cybersecurity council must include:

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

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

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

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

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

28 (d) The cybersecurity council shall:

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

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

3 (3) consolidate and synthesize best practices to
4 assist state agencies in understanding and implementing
5 cybersecurity measures that are most beneficial to this state;
6 and

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

12 (e) The cybersecurity council shall provide
13 recommendations to the legislature on any legislation necessary
14 to implement cybersecurity best practices and remediation
15 strategies for this state.

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

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

25 SECTION 11. Subchapter N-1, Chapter 2054, Government Code,
26 is amended by adding Sections 2054.515, 2054.516, 2054.517, and
27 2054.518 to read as follows:

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

1 storage systems, digital data security measures, and information
2 resources vulnerabilities.

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

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

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

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

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

23 Sec. 2054.517. DATA SECURITY PROCEDURES FOR ONLINE AND
24 MOBILE APPLICATIONS OF INSTITUTIONS OF HIGHER EDUCATION. (a)
25 Each institution of higher education, as defined by Section
26 61.003, Education Code, shall adopt and implement a policy for
27 Internet website and mobile application security procedures that
28 complies with this section.

29 (b) Before deploying an Internet website or mobile
30 application that processes confidential information for an
31 institution of higher education, the developer of the website or

1 application for the institution must submit to the institution's
2 information security officer the information required under
3 policies adopted by the institution to protect the privacy of
4 individuals by preserving the confidentiality of information
5 processed by the website or application. At a minimum, the
6 institution's policies must require the developer to submit
7 information describing:

8 (1) the architecture of the website or application;

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

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

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

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

22 Sec. 2054.518. CYBERSECURITY RISKS AND INCIDENTS. (a)
23 The department shall develop a plan to address cybersecurity
24 risks and incidents in this state. The department may enter
25 into an agreement with a national organization, including the
26 National Cybersecurity Preparedness Consortium, to support the
27 department's efforts in implementing the components of the plan
28 for which the department lacks resources to address internally.
29 The agreement may include provisions for:

30 (1) providing fee reimbursement for appropriate
31 industry-recognized certification examinations for and training

1 to state agencies preparing for and responding to cybersecurity
2 risks and incidents;

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

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

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

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

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

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

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

29 (c) In selecting an organization under Subsection (a), the
30 department shall consider the organization's previous experience
31 in conducting cybersecurity training and exercises for state

1 agencies and political subdivisions.

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

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

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

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

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

19 (3) analysis of the percentage of state agency
20 personnel in information technology, cybersecurity, or other
21 cyber-related positions who currently hold the appropriate
22 industry-recognized certifications as identified by the National
23 Initiative for Cybersecurity Education;

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

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

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

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

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

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

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

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

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

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

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

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

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

1 (b) The study must include:

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

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

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

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

14 (d) This section expires January 1, 2019.

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

19 (1) cybersecurity in this state;

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

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

24 (b) Not later than November 30, 2017:

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

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

31 (c) The committees established under this section shall

1 convene separately at the call of the chair of the respective
2 committees, or jointly at the call of both chairs. In joint
3 meetings, the chairs of each committee shall act as joint
4 chairs.

5 (d) Following consideration of the issues listed in
6 Subsection (a) of this section, the committees established under
7 this section shall jointly adopt recommendations on state
8 cybersecurity and report in writing to the legislature any
9 findings and adopted recommendations not later than January 13,
10 2019.

11 (e) This section expires September 1, 2019.

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

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

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

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

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

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

1 policies;

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

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

7 (6) possible solutions and improvements recommended
8 by the state agencies for reducing state costs and increasing
9 security for digital data storage and records management; and

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

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

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

24 (f) This section expires September 1, 2019.

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

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

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

May 25, 2017

TO: Honorable Joe Straus, Speaker of the House, House of Representatives

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: HB8 by Capriglione (Relating to cybersecurity for state agency information resources.),
As Passed 2nd House

The statewide fiscal implications of the bill cannot be determined at this time, but it is expected to result in a cost to the State. These costs primarily relate to provisions that would require agencies to conduct a risk assessment every two years and periodic vulnerability and penetration tests before deploying certain website or mobile applications.

The bill sets forth certain requirements all agencies would be required to follow relating to cybersecurity. Statewide costs cannot be determined because the impact would be contingent on factors such as an agency's existing information technology infrastructure, current practices, and the number of full-time equivalent positions currently supporting related services. Some agencies such as Texas A&M University and the Texas Department of Transportation estimate an indeterminate but significant cost would be incurred to comply with the requirements of the bill.

The bill also sets forth requirements that would only be applicable to certain agencies. The Sunset Advisory Commission would be required to assess agency cybersecurity practices as part of their reviews, which the Commission estimates would cost \$229,890 in General Revenue Funds during the 2018-19 biennium, including 1.0 additional FTE to provide relevant subject matter expertise. This analysis assumes the Department of Information Resources (DIR) would have an estimated cumulative cost of \$2.2 million and 2.0 additional FTEs for the 2018-19 biennium as a result of requirements to develop plans to address cybersecurity risks and incidents. According to DIR, costs would be funded through the Clearing Fund (Appropriated Receipts), which is generated through administrative fees charged to purchases made through DIR's Cooperative Contracts program. Entities that make purchases through the Cooperative Contracts program include state agencies, institutions of higher education, and local jurisdictions. This analysis assumes that if appropriations do not cover the cost of implementation, DIR would increase administrative fee rates to generate sufficient revenues.

The bill would require DIR to provide mandatory guidelines for all state agency information resources employees regarding continuing education for cybersecurity training and certification. The fiscal impact of continuing education would depend on the training requirements developed by DIR. Agencies such as Trusteed Programs within the Office of the Governor (Trusteed Programs) and the Health and Human Services Commission reported costs associated with ongoing training requirements could be absorbed within existing resources. The Texas Workforce Commission reported 272.0 FTEs perform IT-related projects and training these staff is estimated to cost \$791,384 in General Revenue Funds for the 2018-19 biennium. It is assumed that training and certification requirements and associated costs would continue in subsequent biennia.

The bill would require each state agency to conduct a security assessment of the agency's information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities at least once every two years. Each state agency would be required to report the results of the assessment to DIR, the Governor, the Lieutenant Governor, and the Speaker of the House of Representatives by December 1 in the year in which the agency conducts the assessment. The bill would require DIR to establish the requirements for the information security assessment and report.

The bill would also require that each agency conduct a vulnerability and penetration test of each state agency's website or mobile application that processes any personally identifiable or confidential information. This provision could have a cost for some agencies, although the amount would depend on the manner in which it is implemented by the agency.

The bill would require DIR to develop a plan to address cybersecurity risks and incidents in the state, and authorizes an agreement with a national organization to support DIR's efforts in implementing components for which the agency lacks resources to address internally. This may include provisions such as providing state agencies training and simulation exercises and assistance in developing emergency plans. DIR indicated that the agency would need 2.0 additional FTEs to accomplish the provisions of the bill, estimated at \$2.2 million for the 2018-19 biennium.

Based on agency responses and LBB staff analysis, it is assumed that other provisions of the bill would not have a significant fiscal impact and could be implemented within existing resources.

The bill would take effect September 1, 2017.

Local Government Impact

According to the Texas Association of Counties, this bill would have no fiscal impact to units of local government.

Source Agencies: 116 Sunset Advisory Commission, 304 Comptroller of Public Accounts, 300 Trusteed Programs Within the Office of the Governor, 313 Department of Information Resources, 320 Texas Workforce Commission, 529 Health and Human Services Commission, 601 Department of Transportation, 710 Texas A&M University System Administrative and General Offices

LBB Staff: UP, CL, MMe, BRi

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

May 19, 2017

TO: Honorable Kelly Hancock, Chair, Senate Committee on Business & Commerce

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: HB8 by Capriglione (Relating to cybersecurity for state agency information resources.),
Committee Report 2nd House, Substituted

The statewide fiscal implications of the bill cannot be determined at this time, but it is expected to result in a cost to the State. These costs primarily relate to provisions that would require agencies to perform an information security risk assessment every two years.

The bill sets forth certain requirements all agencies would be required to follow relating to cybersecurity. Statewide costs cannot be determined because the impact would be contingent on factors such as an agency's existing information technology infrastructure, current practices, and the number of full-time equivalent positions currently supporting related services. Some agencies such as Texas A&M University and the Texas Department of Transportation estimate an indeterminate but significant cost would be incurred to comply with the requirements of the bill. The University of Texas System Administration reported that the provisions of the bill could be implemented within existing resources.

The bill would require each state agency to conduct a security assessment of the agency's information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities at least once every two years. Each state agency would be required to report the results of the assessment to DIR, the Governor, the Lieutenant Governor, and the Speaker of the House of Representatives by December 1 in the year in which the agency conducts the assessment. The bill would require DIR to establish the requirements for the information security assessment and report.

The bill would require a state agency to destroy or arrange for the destruction of information that alone or in conjunction with other information presents a cybersecurity risk and alone or in conjunction with other information identifies an individual, if retention of the information is not required under law or for other legal reasons. The cost of this would vary based on how much personally identifiable information an agency retains and what related activities an agency currently undertakes. DIR indicated this could be absorbed within existing resources and the Texas Medical Board estimated this would cost \$50,000 in fiscal year 2019.

Based on agency responses and LBB staff analysis, it is assumed that other provisions of the bill would not have a significant fiscal impact and could be implemented within existing resources.

The bill would take effect September 1, 2017.

Local Government Impact

According to the Texas Association of Counties, this bill would have no fiscal impact to units of local government.

Source Agencies: 116 Sunset Advisory Commission, 300 Trusteed Programs Within the Office of the Governor, 304 Comptroller of Public Accounts, 306 Library & Archives Commission, 307 Secretary of State, 313 Department of Information Resources, 320 Texas Workforce Commission, 323 Teacher Retirement System, 405 Department of Public Safety, 503 Texas Medical Board, 515 Board of Pharmacy, 529 Health and Human Services Commission, 578 Board of Veterinary Medical Examiners, 601 Department of Transportation, 701 Texas Education Agency, 710 Texas A&M University System Administrative and General Offices, 720 The University of Texas System Administration, 781 Higher Education Coordinating Board

LBB Staff: UP, CL, MMe, BRi, RC, JGA

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

May 10, 2017

TO: Honorable Kelly Hancock, Chair, Senate Committee on Business & Commerce

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: HB8 by Capriglione (Relating to cybersecurity for state agency information resources.),
As Engrossed

The statewide fiscal implications of the bill cannot be determined at this time, but it is expected to result in a cost to the State. These costs primarily relate to provisions that would require agencies to contract with an independent third party to perform a risk assessment every five years and periodic vulnerability and penetration tests before deploying certain website or mobile applications.

The bill sets forth certain requirements all agencies would be required to follow relating to cybersecurity. Statewide costs cannot be determined because the impact would be contingent on factors such as an agency's existing information technology infrastructure, current practices, and the number of full-time equivalent (FTE) positions currently supporting related services. Some agencies such as Texas A&M University and the Texas Department of Transportation (TxDOT) estimate an indeterminate but significant cost would be incurred to comply with the requirements of the bill. The University of Texas System Administration reported a cumulative cost of \$6.0 million in General Revenue Funds, \$1.4 million in Available University Funds and an additional 13.2 FTEs would be required in the 2018-19 biennium to accomplish the provisions of the bill.

The bill also sets forth requirements that would only be applicable to certain agencies. The Sunset Advisory Commission would be required to assess agency cybersecurity practices as part of their reviews, which the Commission estimates would cost \$229,890 in General Revenue Funds during the 2018-19 biennium, including 1.0 additional FTE to provide relevant subject matter expertise. This analysis assumes the Department of Information Resources (DIR) would have an estimated cumulative cost of \$5.2 million and 2.0 additional FTEs for the 2018-19 biennium as a result of requirements to develop plans to address cybersecurity risks and incidents. Additionally, if agencies were to utilize DIR's existing third party independent risk assessment services and website and application vulnerability and penetration testing services, the agency estimates an additional cost of \$4.0 million for the biennium to expand current offerings of these services. All costs would be funded through the Clearing Fund (Appropriated Receipts), which is generated through administrative fees charged to purchases made through DIR's Cooperative Contracts program. Entities that make purchases through the Cooperative Contracts program include state agencies, institutions of higher education, and local jurisdictions. This analysis assumes DIR would increase administrative fee rates to generate sufficient revenues to cover the costs of implementation.

The bill would require DIR to provide mandatory guidelines for all state agency information resources employees regarding continuing education for cybersecurity training and certification.

The fiscal impact of continuing education would depend on the training requirements developed by DIR. Agencies such as Trusteed Programs within the Office of the Governor (Trusteed Programs) and the Health and Human Services Commission reported costs associated with ongoing training requirements could be absorbed within existing resources. The Texas Workforce Commission reported 272.0 FTEs perform IT-related projects and training these staff is estimated to cost \$791,384 in General Revenue Funds for the 2018-19 biennium. It is assumed that training and certification requirements and associated costs would continue in subsequent biennia.

The bill would require each state agency to contract at least every five years with an independent third party to conduct and submit to DIR a risk assessment of exposure to security risks. The fiscal impact of this provision would depend on DIR's certification of contractors and the scope and requirements DIR develops for the risk assessment. Agencies provided a variety of estimates regarding potential costs for these risk assessments. Trusteed Programs estimated a cost of \$50,000 in General Revenue Funds per assessment and the University of Texas System estimated costs of \$150,000 to \$350,000 per institution. It is assumed these costs would repeat in subsequent five-year periods.

The bill would also require that an independent third party conduct a vulnerability and penetration test of each state agency's (other than an institution higher education) website or mobile application that processes any personally identifiable or confidential information. The Comptroller of Public Accounts estimated third party contracting costs would be \$750,000 per year and require 1.0 additional FTE for the agency's approximately 88 website applications processing confidential taxpayer information.

DIR indicated it could extend its risk assessment programs to include all agencies and institutions of higher education. If agencies or institutions were to use DIR to accomplish the provisions of the bill related to third party testing requirements, DIR reports that third party costs for up to 48 tests per year could be absorbed under their current contract model. DIR estimates a potential cost of \$4.0 million to agencies in the biennium, were agencies to choose to use a standardized framework developed by DIR for both risk assessment and testing requirements. This assumes that 187 independent risk assessments would be performed over a five year period at a cost of \$48,000 per assessment, and that 20 mobile and application vulnerability tests would be performed per year, at a cost of \$10,000 per test.

The bill would require DIR to develop a plan to address cybersecurity risks and incidents in the state, and authorizes an agreement with a national organization to support DIR's efforts in implementing components for which the agency lacks resources to address internally. This may include provisions such as providing state agencies training and simulation exercises and assistance in developing emergency plans. DIR indicated that the agency would need 2.0 additional FTEs to accomplish the provisions of the bill, estimated at \$5.2 million for the 2018-19 biennium.

The bill would require a state agency to destroy or arrange for the destruction of information that alone or in conjunction with other information presents a cybersecurity risk and alone or in conjunction with other information identifies an individual, if retention of the information is not required under law or for other legal reasons. The cost of this would vary based on how much personally identifiable information an agency retains and what related activities an agency currently undertakes. DIR indicated this could be absorbed within existing resources, the Texas Medical Board estimated this would cost \$50,000 in fiscal year 2019 and DPS reported that 3.0 additional FTEs at a cost of \$697,925 would be required for the 2018-19 biennium.

Based on agency responses and LBB staff analysis, it is assumed that other provisions of the bill

would not have a significant fiscal impact and could be implemented within existing resources.

The bill would take effect September 1, 2017.

Local Government Impact

According to DIR, estimated costs of certification examinations for and training to state and local officials and first responders preparing for and responding to cybersecurity risks and incidents could be \$3.2 million for the biennium, assuming 1,081 school districts, 900 cities and 256 counties at \$2,000 per year. One employee training and certification exam would be conducted per year for one-third of these entities. DIR assumes the cost for the certification examinations and training would be paid out of DIR's Clearing Fund (Appropriated Receipts).

Source Agencies: 116 Sunset Advisory Commission, 300 Trusted Programs Within the Office of the Governor, 304 Comptroller of Public Accounts, 306 Library & Archives Commission, 307 Secretary of State, 313 Department of Information Resources, 320 Texas Workforce Commission, 503 Texas Medical Board, 601 Department of Transportation, 710 Texas A&M University System Administrative and General Offices, 781 Higher Education Coordinating Board, 323 Teacher Retirement System, 405 Department of Public Safety, 515 Board of Pharmacy, 529 Health and Human Services Commission, 578 Board of Veterinary Medical Examiners, 701 Texas Education Agency, 720 The University of Texas System Administration

LBB Staff: UP, CL, MMe, PM, LBO, JAW, RC, LCO, GGo, GO

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

April 14, 2017

TO: Honorable Gary Elkins, Chair, House Committee on Government Transparency & Operation

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: HB8 by Capriglione (Relating to cybersecurity for state agency information resources.),
Committee Report 1st House, Substituted

The statewide fiscal implications of the bill cannot be determined at this time, but is expected to result in a cost to the State. These costs primarily relate to provisions that would require agencies to contract with an independent third party to perform a risk assessment every five years and periodic vulnerability and penetration tests before deploying certain website or mobile applications.

The bill sets forth certain requirements all agencies would be required to follow relating to cybersecurity. Statewide costs cannot be determined because the impact would be contingent on factors such as an agency's existing information technology infrastructure, current practices, and the number of full-time equivalent (FTE) positions currently supporting related services. Some agencies such as Texas A&M University and the Texas Department of Transportation (TxDOT) estimate an indeterminate but significant cost would be incurred to comply with the requirements of the bill. The University of Texas System Administration reported a cumulative cost of \$6.0 million in General Revenue Funds, \$1.4 million in Available University Funds and an additional 13.2 FTEs would be required in the 2018-19 biennium to accomplish the provisions of the bill.

The bill also sets forth requirements that would only be applicable to certain agencies. The Sunset Advisory Commission would be required to assess agency cybersecurity practices as part of their reviews, which the Commission estimates would cost \$229,890 in General Revenue Funds during the 2018-19 biennium, including 1.0 additional FTE to provide relevant subject matter expertise. Requirements that would apply to the Department of Public Safety (DPS) and Department of Information Resources (DIR) are noted below. Based on LBB staff analysis, the cumulative impact to DPS would be a cost of \$6.1 million in General Revenue Funds, including an additional 3.0 FTEs, and certain requirements would have significant yet indeterminate costs. No significant fiscal impact is assumed for DIR to accomplish the bill's requirements of them specifically.

The bill would require DPS to develop a plan to address cybersecurity risks and incidents in the state, and authorizes an agreement with a national organization to support DPS' efforts in implementing components for which the agency lacks resources to address internally. This may include provisions such as providing state agencies training and simulation exercises and assistance in developing emergency plans. Based on LBB staff analysis, DPS would require 3.0 additional FTEs to accomplish these provisions at a cost of approximately \$0.7 million in General Revenue Funds for the 2018-19 biennium. This analysis assumes DPS would provide fee reimbursement for appropriate industry-recognized certification examinations under the

agreement. According to DPS staff, this would cost an additional \$5.2 million in General Revenue Funds, assuming \$20 per certification for 260,000 responders.

The bill would require DIR to provide mandatory guidelines for all state agency information resources employees regarding continuing education for cybersecurity training and certification. The fiscal impact of continuing education would depend on the training requirements developed by DIR. Agencies such as Trusteed Programs within the Office of the Governor (Trusteed Programs) and the Health and Human Services Commission reported costs associated with ongoing training requirements could be absorbed within existing resources. The Texas Workforce Commission reported 272 FTEs perform IT-related projects and training these staff is estimated to cost \$791,384 in General Revenue Funds for the 2018-19 biennium. It is assumed that training and certification requirements and associated costs would continue in subsequent biennia.

The bill would require each state agency to contract at least every five years with an independent third party to conduct and submit to DIR a risk assessment of exposure to security risks. The fiscal impact of this provision would depend on DIR's certification of contractors and the scope and requirements DIR develops for the risk assessment. Agencies provided a variety of estimates regarding potential costs for these risk assessments. Trusteed Programs estimated a cost of \$50,000 in General Revenue Funds per assessment and the University of Texas System estimated costs of \$150,000 to \$350,000 per institution. It is assumed these costs would repeat in subsequent five-year periods.

The bill would also require that each state agency (other than an institution higher education) website or mobile application processing any personally identifiable or confidential information undergo a vulnerability and penetration test conducted by an independent third party. The Comptroller of Public Accounts estimated third party contracting costs would be \$750,000 per year and require 1.0 additional FTE for the agency's approximately 88 website applications processing confidential taxpayer information.

DIR indicated it could extend its risk assessment programs to include all agencies and institutions of higher education. If agencies or institutions were to use DIR to accomplish the provisions of the bill related to third party testing requirements, DIR reports that third party costs for up to 48 tests per year could be absorbed under their current contract model. DIR estimates a potential cost of \$4.0 million in the biennium were agencies to choose to use a standardized framework developed by DIR for both risk assessment and testing requirements, and assumes this would include 20 new vulnerability tests per year at a cost of \$10,000 per test.

The bill would require a state agency to destroy or arrange for the destruction of information that alone or in conjunction with other information presents a cybersecurity risk and alone or in conjunction with other information identifies an individual, if retention of the information is not required under law or for other legal reasons. The cost of this would vary based on how much personally identifiable information an agency retains and what related activities an agency currently undertakes. DIR indicated this could be absorbed within existing resources, the Texas Medical Board estimated this would cost \$50,000 in fiscal year 2019 and DPS stated the costs related to Intelligence and Counterterrorism Division and Homeland Security responsibilities would be significant but cannot be determined.

Based on agency responses and LBB staff analysis, it is assumed that other provisions of the bill would not have a significant fiscal impact and could be implemented within existing resources.

The bill would take effect September 1, 2017.

Local Government Impact

No fiscal implication to units of local government is anticipated.

Source Agencies: 306 Library & Archives Commission, 307 Secretary of State, 710 Texas A&M University System Administrative and General Offices, 781 Higher Education Coordinating Board, 116 Sunset Advisory Commission, 300 Trusteed Programs Within the Office of the Governor, 304 Comptroller of Public Accounts, 313 Department of Information Resources, 320 Texas Workforce Commission, 323 Teacher Retirement System, 405 Department of Public Safety, 503 Texas Medical Board, 515 Board of Pharmacy, 529 Health and Human Services Commission, 578 Board of Veterinary Medical Examiners, 601 Department of Transportation, 701 Texas Education Agency, 720 The University of Texas System Administration

LBB Staff: UP, LBO, MMe, PM, JAW, RC, LCO, GGo, GO

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

March 20, 2017

TO: Honorable Gary Elkins, Chair, House Committee on Government Transparency & Operation

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: HB8 by Capriglione (Relating to cybersecurity for state agency information resources.),
As Introduced

The statewide fiscal implications of the bill cannot be determined at this time, but is expected to result in a cost to the State. These costs primarily relate to provisions that would require agencies to contract with an independent third party to perform a risk assessment every five years and periodic vulnerability and penetration tests before deploying certain website or mobile applications.

The bill sets forth certain requirements all agencies would be required to follow relating to cybersecurity. The costs cannot be determined because the impact would be contingent on factors such as an agency's existing information technology infrastructure, current practices, and the number of full-time equivalent (FTE) positions currently supporting related services. Some agencies such as Texas A&M University and the Texas Department of Transportation (TxDOT) estimate an indeterminate but significant cost would be incurred to comply with the requirements of the bill. The University of Texas System Administration reported a cumulative cost of \$22.6 million in General Revenue Funds, \$1.3 million in Available University Funds and an additional 13.2 FTEs would be required in the 2018-19 biennium to accomplish the provisions of the bill.

The bill also sets forth requirements that would only be applicable to certain agencies. The Sunset Advisory Commission would be required to assess agency cybersecurity practices as part of their reviews, which the Commission estimates would cost \$229,890 in General Revenue Funds during the 2018-19 biennium, including 1.0 additional FTE. Requirements that would apply to the Department of Public Safety (DPS) and Department of Information Resources (DIR) are noted below. Based on LBB staff analysis, the cumulative impact to DPS would be an additional 4.0 FTEs at a cost of \$1.0 million in General Revenue Funds, and certain requirements would have significant yet indeterminate costs. No significant fiscal impact is assumed for DIR to accomplish the bill's requirements of them specifically.

The bill would authorize DPS to enter into an agreement with a national organization to address cybersecurity risks and incidents in the state, and authorizes an agreement with an organization to include certain provisions such as providing state agencies training and simulation exercises and assistance in developing emergency plans. Based on LBB staff analysis, DPS would require 3.0 additional FTEs to accomplish these provisions at a cost of approximately \$0.7 million in General Revenue Funds for the 2018-19 biennium.

The bill would require the Homeland Security Council conduct a one-time study regarding cyber

attacks on state agencies and critical infrastructure, and develop a plan agencies would implement in the event of a cyber attack. Based on LBB staff analysis, DPS would incur a one-time cost of approximately \$86,647 for 1.0 additional FTE, plus benefits, to assist the Council in completing this requirement.

The bill would require DIR to provide mandatory guidelines for all state agency information resources employees regarding continuing education for cybersecurity training and certification. The fiscal impact of continuing education would depend on the training requirements developed by DIR. Agencies such as Trusteed Programs within the Office of the Governor (Trusteed Programs) and the Health and Human Services Commission reported costs associated with ongoing training requirements could be absorbed within existing resources. The Texas Workforce Commission reported 272 FTEs perform IT-related projects and training these staff is estimated to cost \$791,384 in General Revenue Funds for the 2018-19 biennium. It is assumed that training and certification requirements and associated costs would continue in subsequent biennia.

The bill would require the executive head and chief information security officer (CISO) of each state agency to annually review the agency's information security plan, develop strategies for information resources systems that are at highest risk for security breaches, and submit these to the Legislative Budget Board. There is no statutory requirement for agencies to have a CISO; therefore some agencies may need additional staff to fulfill this requirement, although the number of additional staff that would be hired is unknown. The average annual salary, without benefits, for a CISO is \$119,847 per year.

The bill would require each state agency to contract at least every five years with an independent third party to conduct and submit to DIR a risk assessment of exposure to security risks. The fiscal impact of this provision would depend on DIR's certification of contractors and the scope and requirements DIR develops for the risk assessment. Agencies provided a variety of estimates regarding potential costs for these risk assessments. Trusteed Programs estimated a cost of \$50,000 in General Revenue Funds per assessment and the University of Texas System estimated costs of \$150,000 to \$350,000 per institution. It is assumed these costs would repeat in subsequent five-year periods.

The bill would also require that each state agency website or mobile application processing any personally identifiable or confidential information undergo a vulnerability and penetration test conducted by an independent third party. UT Austin indicated they currently perform 20 to 25 of these types of tests each month in-house. At an estimated \$10,000 per external test, they estimate a cost of \$2.4 million annually to expand this testing to meet the third party contract requirements of the bill. The Comptroller of Public Accounts estimated third party contracting costs would be \$750,000 per year and require 1.0 additional FTE for the agency's approximately 88 website applications processing confidential taxpayer information.

DIR indicated it could extend its risk assessment programs to include all agencies and institutions of higher education. If agencies or institutions were to use DIR to accomplish the provisions of the bill related to third party testing requirements, DIR reports that third party costs for up to 48 tests per year could be absorbed under their current contract model. DIR estimates a potential cost of \$4.0 million in the biennium were agencies to choose to use a standardized framework developed by DIR for both risk assessment and testing requirements, and assumes this would include 20 new vulnerability tests per year at a cost of \$10,000 per test.

The bill would require a state agency to destroy or arrange for the destruction of information that alone or in conjunction with other information identifies an individual, if retention of the information is not required under other law. The cost of this would vary based on how much

personally identifiable information an agency retains and what related activities an agency currently undertakes. DIR indicated this could be absorbed within existing resources, the Texas Medical Board estimated this would cost \$50,000 in fiscal year 2019, and DPS stated the cost would be significant but cannot be determined.

The bill would require the Texas Rangers conduct a one-time study regarding cyber attacks on election infrastructure. DPS staff stated the cost for this would be significant but cannot be determined.

Based on agency responses and LBB staff analysis, it is assumed that other provisions of the bill would not have a significant fiscal impact and could be implemented within existing resources.

The bill would take effect September 1, 2017.

Local Government Impact

No fiscal implication to units of local government is anticipated.

Source Agencies: 116 Sunset Advisory Commission, 300 Trusteed Programs Within the Office of the Governor, 304 Comptroller of Public Accounts, 306 Library & Archives Commission, 313 Department of Information Resources, 320 Texas Workforce Commission, 323 Teacher Retirement System, 405 Department of Public Safety, 503 Texas Medical Board, 515 Board of Pharmacy, 529 Health and Human Services Commission, 578 Board of Veterinary Medical Examiners, 601 Department of Transportation, 701 Texas Education Agency, 710 Texas A&M University System Administrative and General Offices, 720 The University of Texas System Administration, 781 Higher Education Coordinating Board

LBB Staff: UP, LBO, MMe, PM, LCO, GGo, GO, RC