

Chapter 955

S.B. No. 1910

AN ACT

relating to state agency information security plans, information technology employees, and online and mobile applications.

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

SECTION 1. Subchapter C, Chapter 2054, Government Code, is amended by adding Sections 2054.0591 and 2054.0592 to read as follows:

Sec. 2054.0591. CYBERSECURITY REPORT. (a) Not later than November 15 of each even-numbered year, the department shall submit to the governor, the lieutenant governor, the speaker of the house of representatives, and the standing committee of each house of the legislature with primary jurisdiction over state government operations a report identifying preventive and recovery efforts the state can undertake to improve cybersecurity in this state. The report must include:

(1) an assessment of the resources available to address the operational and financial impacts of a cybersecurity event;

(2) a review of existing statutes regarding cybersecurity and information resources technologies;

(3) recommendations for legislative action to increase the state's cybersecurity and protect against adverse impacts from a cybersecurity event;

(4) an evaluation of the costs and benefits of

1 cybersecurity insurance; and

2 (5) an evaluation of tertiary disaster recovery
3 options.

4 (b) The department or a recipient of a report under this
5 section may redact or withhold information confidential under
6 Chapter 552, including Section 552.139, or other state or federal
7 law that is contained in the report in response to a request under
8 Chapter 552 without the necessity of requesting a decision from the
9 attorney general under Subchapter G, Chapter 552.

10 Sec. 2054.0592. CYBERSECURITY EMERGENCY FUNDING. If a
11 cybersecurity event creates a need for emergency funding, the
12 department may request that the governor or Legislative Budget
13 Board make a proposal under Chapter 317 to provide funding to manage
14 the operational and financial impacts from the cybersecurity event.

15 SECTION 2. Subchapter F, Chapter 2054, Government Code, is
16 amended by adding Section 2054.1184 to read as follows:

17 Sec. 2054.1184. ASSESSMENT OF MAJOR INFORMATION RESOURCES
18 PROJECT. (a) A state agency proposing to spend appropriated funds
19 for a major information resources project must first conduct an
20 execution capability assessment to:

21 (1) determine the agency's capability for implementing
22 the project;

23 (2) reduce the agency's financial risk in implementing
24 the project; and

25 (3) increase the probability of the agency's
26 successful implementation of the project.

27 (b) A state agency shall submit to the department, the

S.B. No. 1910

1 quality assurance team established under Section 2054.158, and the
2 Legislative Budget Board a detailed report that identifies the
3 agency's organizational strengths and any weaknesses that will be
4 addressed before the agency initially spends appropriated funds for
5 a major information resources project.

6 (c) A state agency may contract with an independent third
7 party to conduct the assessment under Subsection (a) and prepare
8 the report described by Subsection (b).

9 SECTION 3. Section 2054.133(c), Government Code, is amended
10 to read as follows:

11 (c) Not later than October 15 of each even-numbered year,
12 each state agency shall submit a copy of the agency's information
13 security plan to the department. Subject to available resources,
14 the department may select a portion of the submitted security plans
15 to be assessed by the department in accordance with department
16 rules.

17 SECTION 4. Subchapter F, Chapter 2054, Government Code, is
18 amended by adding Section 2054.136 to read as follows:

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

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

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

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

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

3 SECTION 5. Subchapter N-1, Chapter 2054, Government Code,
4 is amended by adding Sections 2054.516 and 2054.517 to read as
5 follows:

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

11 (1) submit a biennial data security plan to the
12 department not later than October 15 of each even-numbered year, to
13 establish planned beta testing for websites or applications; and

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

17 (b) The department shall review each data security plan
18 submitted under Subsection (a) and make any recommendations for
19 changes to the plan to the state agency as soon as practicable after
20 the department reviews the plan.

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

27 (b) Before deploying an Internet website or mobile

S.B. No. 1910

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

- 10 (1) the architecture of the website or application;
11 (2) the authentication mechanism for the website or
12 application; and
13 (3) the administrator-level access to data included in
14 the website or application.

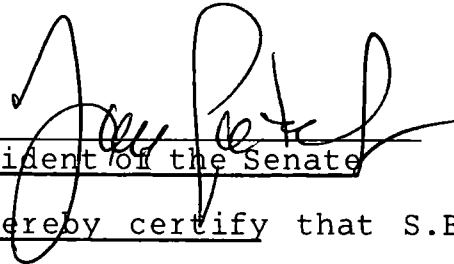
15 (c) Before deploying an Internet website or mobile
16 application described by Subsection (b), an institution of higher
17 education must subject the website or application to a
18 vulnerability and penetration test conducted internally or by an
19 independent third party.

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

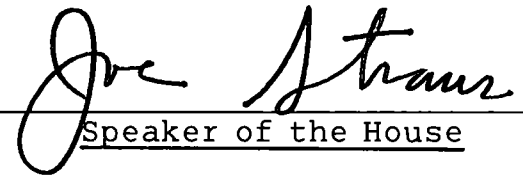
24 SECTION 6. As soon as practicable after the effective date
25 of this Act, the Department of Information Resources shall adopt
26 the rules necessary to implement Section 2054.133(c), Government
27 Code, as amended by this Act.

S.B. No. 1910

1 SECTION 7. This Act takes effect September 1, 2017. _____

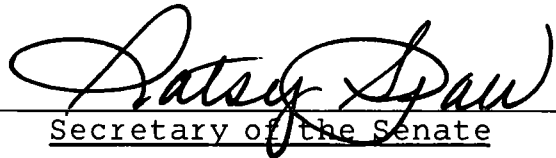


President of the Senate



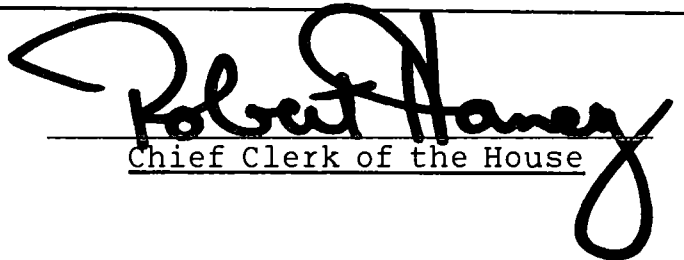
Speaker of the House

I hereby certify that S.B. No. 1910 passed the Senate on May 4, 2017, by the following vote: Yeas 31, Nays 0; and that the Senate concurred in House amendments on May 26, 2017, by the following vote: Yeas 31, Nays 0. _____



Secretary of the Senate

I hereby certify that S.B. No. 1910 passed the House, with amendments, on May 22, 2017, by the following vote: Yeas 144, Nays 0, one present not voting. _____



Chief Clerk of the House

Approved:

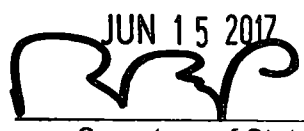
6-12-2017

Date



Governor

FILED IN THE OFFICE OF THE
SECRETARY OF STATE
3 PM O'CLOCK

JUN 15 2017


Secretary of State

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

May 23, 2017

TO: Honorable Dan Patrick, Lieutenant Governor, Senate

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: SB1910 by Zaffirini (Relating to state agency information security plans, information technology employees, and online and mobile applications.), **As Passed 2nd House**

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 of the bill that would require agencies to perform vulnerability and penetration tests before deploying certain website or mobile applications.

The bill would amend Chapter 2054, Government Code, to authorize the Department of Information Resources (DIR) to select a portion of the security plans submitted to DIR under Section 2054.133 to be assessed by DIR, subject to available resources. The bill would require each state agency to designate an information security officer within the agency.

The bill would require each state agency implementing an Internet website or mobile application that processes any personally identifiable or confidential information to submit a biennial data security plan to DIR; to subject the website or application to a vulnerability and penetration test; and to address any vulnerability identified. The bill would require DIR to review and make recommendations for changes to the plan.

The bill would require institutions of higher education to adopt and implement a policy for internet website and mobile application security procedures. The bill would require the institutions to subject the websites or applications which would process confidential information to a vulnerability and penetration test prior to the deployments.

The bill would require DIR to submit to certain leadership and committees of the Legislature a biennial report identifying preventive and recovery efforts the state can undertake to improve cybersecurity in this state. If a cybersecurity event creates the need for emergency funding, the bill would authorize DIR to request that the Governor or Legislative Budget Board make a proposal under Chapter 317, related to state budget execution, to provide funding to manage the impacts from the cybersecurity event.

The bill would require agencies to assess their capability to execute major information resource projects before spending funds on such projects. Assessments of an agency's strengths and weaknesses in executing such projects would be submitted to the Department of Information Resources, the Quality Assurance Team, and the Legislative Budget Board.

The bill sets forth certain requirements all agencies would be required to follow relating to information technology security. 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.

Agencies indicated various costs to implement requirements for data security plans and for vulnerability and penetration tests before online and mobile applications are deployed. The Office of the Attorney General indicates that six applications would be tested annually for a total of \$90,000 each fiscal year out of General Revenue and Federal Funds. The General Land Office indicated a total of \$84,000 for each fiscal year in General Revenue for contractor costs due to longer project implementation timelines, testing requirements, resolution of test issues and training. Additionally, the Texas A&M University System estimates there would be a cost to implement the testing requirements. Other agencies, such as the Office of the Governor, Board of Nursing, and Department of Licensing and Regulation indicate that costs could be absorbed within existing resources.

This analysis assumes that agencies which do not currently employ an information security officer could designate a current employee to meet the provisions of Section 2054.136, as added by the bill.

DIR indicates that their costs to implement the bills provisions could be absorbed within existing resources.

Local Government Impact

No fiscal implication to units of local government is anticipated.

Source Agencies: 300 Trusteed Programs Within the Office of the Governor, 305 General Land Office and Veterans' Land Board, 312 Securities Board, 313 Department of Information Resources, 452 Department of Licensing and Regulation, 507 Texas Board of Nursing, 582 Commission on Environmental Quality, 608 Department of Motor Vehicles, 644 Juvenile Justice Department, 710 Texas A&M University System Administrative and General Offices, 302 Office of the Attorney General, 529 Health and Human Services Commission, 720 The University of Texas System Administration

LBB Staff: UP, AG, NV, LCO, RC, CL, WP, PM

**LEGISLATIVE BUDGET BOARD
Austin, Texas**

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

April 20, 2017

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

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: SB1910 by Zaffirini (Relating to state agency information security plans, information technology employees, and online and mobile applications.), **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 of the bill that would require DIR to audit agency information security plans and requirements for agencies to contract with an independent third party to perform vulnerability and penetration tests before deploying certain website or mobile applications.

The bill would amend Chapter 2054, Government Code, to require the Department of Information Resources (DIR) to select a portion of the security plans submitted to DIR under Section 2054.133 to be audited by DIR, subject to available resources. The bill would require each state agency in the executive branch that has on staff a chief information security officer or an information security officer to ensure that the officer is independent from and not subordinate to the agency's information technology operations.

The bill would require each state agency implementing an Internet website or mobile application that processes any personally identifiable or confidential information to submit a data security plan to DIR and to subject the website or application to a vulnerability and penetration test conducted by an independent third party and address any vulnerability identified. The bill would specify the information to be included in the data security plan and would require DIR to review and make recommendations for changes to the plan.

The bill sets forth certain requirements all agencies would be required to follow relating to information technology security. 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.

DIR indicates a cost of \$900,000 annually, from the Clearing Fund (Other Funds) to perform audits for an estimated 15 security plans annually at a cost of \$60,000 per audit.

Agencies indicated various costs to implement requirements for data security plans and for vulnerability and penetration tests conducted by an independent third party before online and mobile applications are deployed. The Office of the Attorney General indicates that six applications would be tested annually for a total of \$90,000 each fiscal year out of General Revenue and Federal Funds. The General Land Office indicated a total of \$84,000 for each fiscal

year in General Revenue for contractor costs due to longer project implementation timelines, testing requirements, resolution of test issues and training. Additionally, the University of Texas System indicated annual costs of \$9,052,867 to \$9,267,468 primarily for testing requirements. Other agencies, such as the Office of the Governor, Board of Nursing, and Health and Human Services Commission indicated that costs could be absorbed within existing resources.

Local Government Impact

No fiscal implication to units of local government is anticipated.

Source Agencies: 300 Trusteed Programs Within the Office of the Governor, 302 Office of the Attorney General, 305 General Land Office and Veterans' Land Board, 312 Securities Board, 313 Department of Information Resources, 452 Department of Licensing and Regulation, 507 Texas Board of Nursing, 529 Health and Human Services Commission, 582 Commission on Environmental Quality, 608 Department of Motor Vehicles, 644 Juvenile Justice Department, 710 Texas A&M University System Administrative and General Offices, 720 The University of Texas System Administration

LBB Staff: UP, CL, WP, LCO, NV, RC, PM

**LEGISLATIVE BUDGET BOARD
Austin, Texas**

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

April 10, 2017

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

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: SB1910 by Zaffirini (Relating to state agency information security plans, information technology employees, and online and mobile applications.), **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 of the bill that would require DIR to audit agency information security plans and requirements for agencies to contract with an independent third party to perform vulnerability and penetration tests before deploying certain website or mobile applications.

The bill would amend Chapter 2054, Government Code, to require the Department of Information Resources (DIR) to select a portion of the security plans submitted to DIR under Section 2054.133 to be audited by DIR. The bill would require that each state agency in the executive branch that has on staff a chief information security officer to ensure that the officer is independent from and not subordinate to the agency's information technology operations.

The bill would require each state agency implementing an Internet website or mobile application that processes any personally identifiable or confidential information to submit a data security plan to DIR and to subject the website or application to a vulnerability and penetration test conducted by an independent third party and address any vulnerability identified. The bill would specify the information to be included in the data security plan and would require DIR to review and make recommendations for changes to the plan.

The bill sets forth certain requirements all agencies would be required to follow relating to information technology security. 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.

DIR indicates a cost of \$900,000 annually, from the Clearing Fund (Other Funds) to perform audits for an estimated 15 security plans annually at a cost of \$60,000 per audit.

Agencies indicated various costs to implement requirements for data security plans and for vulnerability and penetration tests conducted by an independent third party before online and mobile applications are deployed. The Office of the Attorney General indicates that six applications would be tested annually for a total of \$90,000 each fiscal year out of General Revenue and Federal Funds. The General Land Office indicated a total of \$84,000 for each fiscal year in General Revenue for contractor costs due to longer project implementation timelines, testing requirements, resolution of test issues and training. Additionally, the University of Texas

System indicated annual costs of \$9,052,867 to \$9,267,468 primarily for testing requirements. Other agencies, such as the Office of the Governor, Board of Nursing, and Health and Human Services Commission indicated that costs could be absorbed within existing resources.

Local Government Impact

No fiscal implication to units of local government is anticipated.

Source Agencies: 300 Trusteed Programs Within the Office of the Governor, 302 Office of the Attorney General, 305 General Land Office and Veterans' Land Board, 312 Securities Board, 313 Department of Information Resources, 452 Department of Licensing and Regulation, 507 Texas Board of Nursing, 529 Health and Human Services Commission, 582 Commission on Environmental Quality, 608 Department of Motor Vehicles, 644 Juvenile Justice Department, 710 Texas A&M University System Administrative and General Offices, 720 The University of Texas System Administration

LBB Staff: UP, CL, NV, LCO, RC, PM