

By: Zaffirini
(Capriglione)

S.B. No. 1910

A BILL TO BE ENTITLED

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

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

SECTION 2. Subchapter F, Chapter 2054, Government Code, is amended by adding Section 2054.136 to read as follows:

Sec. 2054.136. INDEPENDENT INFORMATION SECURITY OFFICER. Each state agency in the executive branch of state government that has on staff a chief information security officer or information security officer shall ensure that within the agency's organizational structure the officer is independent from and not subordinate to the agency's information technology operations.

SECTION 3. Subchapter N-1, Chapter 2054, Government Code, is amended by adding Section 2054.516 to read as follows:

Sec. 2054.516. DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS. (a) Each state agency implementing an Internet

1 website or mobile application that processes any personally
2 identifiable or confidential information must:

3 (1) submit a data security plan to the department
4 before beta testing the website or application; and

5 (2) before deploying the website or application:

6 (A) subject the website or application to a
7 vulnerability and penetration test conducted by an independent
8 third party; and

9 (B) address any vulnerability identified under
10 Paragraph (A).

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

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

15 (2) data storage locations;

16 (3) data interaction with online or mobile devices;

17 (4) security of data transfer;

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

20 (6) a description of any action taken by the agency to
21 remediate any vulnerability identified by an independent third
22 party under Subsection (a)(2).

23 (c) The department shall review each data security plan
24 submitted under Subsection (a) and make any recommendations for
25 changes to the plan to the state agency as soon as practicable after
26 the department reviews the plan.

27 SECTION 4. As soon as practicable after the effective date

1 of this Act, the Department of Information Resources shall adopt
2 the rules necessary to implement Section [2054.133\(c\)](#), Government
3 Code, as amended by this Act.

4 SECTION 5. This Act takes effect September 1, 2017.