

1-1 By: Zaffirini S.B. No. 1910  
 1-2 (In the Senate - Filed March 10, 2017; March 23, 2017, read  
 1-3 first time and referred to Committee on Business & Commerce;  
 1-4 April 24, 2017, reported adversely, with favorable Committee  
 1-5 Substitute by the following vote: Yeas 8, Nays 0; April 24, 2017,  
 1-6 sent to printer.)

1-7 COMMITTEE VOTE

	Yea	Nay	Absent	PNV
1-8				
1-9	X			
1-10	X			
1-11	X			
1-12	X			
1-13	X			
1-14	X			
1-15	X			
1-16			X	
1-17	X			

1-18 COMMITTEE SUBSTITUTE FOR S.B. No. 1910 By: Campbell

1-19 A BILL TO BE ENTITLED  
 1-20 AN ACT

1-21 relating to state agency information security plans, information  
 1-22 technology employees, and online and mobile applications.

1-23 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

1-24 SECTION 1. Section 2054.133(c), Government Code, is amended  
 1-25 to read as follows:

1-26 (c) Not later than October 15 of each even-numbered year,  
 1-27 each state agency shall submit a copy of the agency's information  
 1-28 security plan to the department. Subject to available resources,  
 1-29 the department shall select a portion of the submitted security  
 1-30 plans to be audited by the department in accordance with department  
 1-31 rules.

1-32 SECTION 2. Subchapter F, Chapter 2054, Government Code, is  
 1-33 amended by adding Section 2054.136 to read as follows:

1-34 Sec. 2054.136. INDEPENDENT INFORMATION SECURITY OFFICER.  
 1-35 Each state agency in the executive branch of state government that  
 1-36 has on staff a chief information security officer or information  
 1-37 security officer shall ensure that within the agency's  
 1-38 organizational structure the officer is independent from and not  
 1-39 subordinate to the agency's information technology operations.

1-40 SECTION 3. Subchapter N-1, Chapter 2054, Government Code,  
 1-41 is amended by adding Section 2054.516 to read as follows:

1-42 Sec. 2054.516. DATA SECURITY PLAN FOR ONLINE AND MOBILE  
 1-43 APPLICATIONS. (a) Each state agency implementing an Internet  
 1-44 website or mobile application that processes any personally  
 1-45 identifiable or confidential information must:

1-46 (1) submit a data security plan to the department  
 1-47 before beta testing the website or application; and

1-48 (2) before deploying the website or application:

1-49 (A) subject the website or application to a  
 1-50 vulnerability and penetration test conducted by an independent  
 1-51 third party; and

1-52 (B) address any vulnerability identified under  
 1-53 Paragraph (A).

1-54 (b) The data security plan required under Subsection (a)(1)  
 1-55 must include:

1-56 (1) data flow diagrams to show the location of  
 1-57 information in use, in transit, and not in use;

1-58 (2) data storage locations;

1-59 (3) data interaction with online or mobile devices;

1-60 (4) security of data transfer;

2-1 (5) security measures for the online or mobile  
2-2 application; and

2-3 (6) a description of any action taken by the agency to  
2-4 remediate any vulnerability identified by an independent third  
2-5 party under Subsection (a)(2).

2-6 (c) The department shall review each data security plan  
2-7 submitted under Subsection (a) and make any recommendations for  
2-8 changes to the plan to the state agency as soon as practicable after  
2-9 the department reviews the plan.

2-10 SECTION 4. As soon as practicable after the effective date  
2-11 of this Act, the Department of Information Resources shall adopt  
2-12 the rules necessary to implement Section 2054.133(c), Government  
2-13 Code, as amended by this Act.

2-14 SECTION 5. This Act takes effect September 1, 2017.

2-15 \* \* \* \* \*