

By: Ellis

S.B. No. 2164

A BILL TO BE ENTITLED

1 AN ACT  
2 relating to information technology security practices of state  
3 agencies.

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

5 SECTION 1. Section 411.081(i), Government Code, is amended  
6 to read as follows:

7 (i) A criminal justice agency may disclose criminal history  
8 record information that is the subject of an order of nondisclosure  
9 to the following noncriminal justice agencies or entities only:

- 10 (1) the State Board for Educator Certification;
- 11 (2) a school district, charter school, private school,  
12 regional education service center, commercial transportation  
13 company, or education shared service arrangement;
- 14 (3) the Texas Medical Board;
- 15 (4) the Texas School for the Blind and Visually  
16 Impaired;
- 17 (5) the Board of Law Examiners;
- 18 (6) the State Bar of Texas;
- 19 (7) a district court regarding a petition for name  
20 change under Subchapter B, Chapter 45, Family Code;
- 21 (8) the Texas School for the Deaf;
- 22 (9) the Department of Family and Protective Services;
- 23 (10) the Texas Youth Commission;
- 24 (11) the Department of Assistive and Rehabilitative

1 Services;

2 (12) the Department of State Health Services, a local  
3 mental health service, a local mental retardation authority, or a  
4 community center providing services to persons with mental illness  
5 or retardation;

6 (13) the Texas Private Security Board;

7 (14) a municipal or volunteer fire department;

8 (15) the Texas Board of Nursing;

9 (16) a safe house providing shelter to children in  
10 harmful situations;

11 (17) a public or nonprofit hospital or hospital  
12 district;

13 (18) the Texas Juvenile Probation Commission;

14 (19) the securities commissioner, the banking  
15 commissioner, the savings and mortgage lending commissioner, or the  
16 credit union commissioner;

17 (20) the Texas State Board of Public Accountancy;

18 (21) the Texas Department of Licensing and Regulation;

19 (22) the Health and Human Services Commission;

20 (23) the Department of Aging and Disability Services;

21 [~~and~~]

22 (24) the Texas Education Agency; and

23 (25) the Texas Department of Information Resources  
24 regarding an employee, applicant for employment, contractor,  
25 subcontractor, intern, or volunteer that provides network security  
26 services under Chapter 2059, Government Code, to:

27 (A) the Department of Information Resources; or

1           (B) a contractor or subcontractor of the  
2 Department of Information Resources.

3           SECTION 2. Subchapter F, Chapter 411, Government Code, is  
4 amended by adding Section 411.1404 to read as follows:

5           Sec. 411.1404. ACCESS TO CRIMINAL HISTORY RECORD  
6 INFORMATION: DEPARTMENT OF INFORMATION RESOURCES. (a) The  
7 Department of Information Resources is entitled to obtain from the  
8 department or the Federal Bureau of Investigation identification  
9 division the criminal history record information maintained by the  
10 department that relates to a person who is an employee, applicant  
11 for employment, contractor, subcontractor, intern, or volunteer of  
12 the Department of Information Resources or a contractor or  
13 subcontractor that provides services to the Department of  
14 Information Resources.

15           (b) Criminal history record information obtained by the  
16 Department of Information Resources under this section may not be  
17 released or disclosed except by court order or with the consent of  
18 the person who is the subject of the information.

19           (c) The Department of Information Resources shall destroy  
20 criminal history record information obtained under this section  
21 that relates to a person after the information is used to make an  
22 employment decision or to take a personnel action relating to the  
23 person who is the subject of the information.

24           (d) The Department of Information Resources may not obtain  
25 criminal history record information under this section unless the  
26 Department of Information Resources first adopts policies and  
27 procedures that provide that evidence of a criminal conviction or

1 other relevant information obtained from the criminal history  
2 record information does not automatically disqualify an individual  
3 from employment. The policies and procedures adopted under this  
4 subsection must provide that the hiring official will determine, on  
5 a case-by-case basis, whether the individual is qualified for  
6 employment based on factors that include:

- 7           (1) the specific duties of the position;  
8           (2) the number of offenses committed by the  
9 individual;  
10           (3) the nature and seriousness of each offense;  
11           (4) the length of time between the offense and the  
12 employment decision;  
13           (5) the efforts by the individual at rehabilitation;  
14 and  
15           (6) the accuracy of the information on the  
16 individual's employment application.

17           SECTION 3. Subchapter D, Chapter 551, Government Code, is  
18 amended by adding Section 551.089 to read as follows:

19           Sec. 551.089. DEPARTMENT OF INFORMATION RESOURCES. This  
20 chapter does not require the governing board of the Department of  
21 Information Resources to conduct an open meeting to deliberate:

- 22           (1) security assessments or deployments relating to  
23 information resources technology;  
24           (2) network security information as described by  
25 Section 2059.055(b); or  
26           (3) the deployment, or specific occasions for  
27 implementation, of security personnel, critical infrastructure, or

1 security devices.

2 SECTION 4. Section 552.139, Government Code, is amended to  
3 read as follows:

4 Sec. 552.139. EXCEPTION: GOVERNMENT INFORMATION RELATED TO  
5 SECURITY OR INFRASTRUCTURE ISSUES FOR COMPUTERS. (a) Information  
6 is excepted from the requirements of Section 552.021 if it is  
7 information that relates to computer network security, to  
8 restricted information under Section 2059.055, or to the design,  
9 operation, or defense of a computer network.

10 (b) The following information is confidential:

- 11 (1) a computer network vulnerability report; and  
12 (2) any other assessment of the extent to which data  
13 processing operations, a computer, [~~or~~] a computer program,  
14 network, system, or system interface, or software of a governmental  
15 body or of a contractor of a governmental body is vulnerable to  
16 unauthorized access or harm, including an assessment of the extent  
17 to which the governmental body's or contractor's electronically  
18 stored information containing sensitive or critical information is  
19 vulnerable to alteration, damage, [~~or~~] erasure, or inappropriate  
20 use.

21 (c) Notwithstanding the confidential nature of the  
22 information described in this section, the information may be  
23 disclosed to a bidder if the governmental body determines that  
24 providing the information is necessary for the bidder to provide an  
25 accurate bid. A disclosure under this subsection is not a voluntary  
26 disclosure for purposes of Section 552.007.

27 SECTION 5. Sections 2054.077(b), (d), and (e), Government

1 Code, are amended to read as follows:

2 (b) The information resources manager of a state agency may  
3 prepare or have prepared a report, including an executive summary  
4 of the findings of the report, assessing the extent to which a  
5 computer, a computer program, a computer network, a computer  
6 system, an interface to a computer system, computer software, or  
7 data processing of the agency or of a contractor of the agency is  
8 vulnerable to unauthorized access or harm, including the extent to  
9 which the agency's or contractor's electronically stored  
10 information is vulnerable to alteration, damage, ~~or~~ erasure, or  
11 inappropriate use.

12 (d) The ~~[On request, the]~~ information resources manager  
13 shall provide an electronic ~~[a]~~ copy of the vulnerability report on  
14 its completion to:

- 15 (1) the department;
- 16 (2) the state auditor; ~~[and]~~
- 17 (3) the agency's executive director; and
- 18 (4) any other information technology security  
19 oversight group specifically authorized by the legislature to  
20 receive the report.

21 (e) Separate from the executive summary described by  
22 Subsection (b), a ~~[A]~~ state agency whose information resources  
23 manager has prepared or has had prepared a vulnerability report  
24 shall prepare a summary of the report that does not contain any  
25 information the release of which might compromise the security of  
26 the state agency's or state agency contractor's computers, computer  
27 programs, computer networks, computer systems, computer software,

1 data processing, or electronically stored information. The summary  
2 is available to the public on request.

3 SECTION 6. This Act takes effect September 1, 2009.