

AN ACT

relating to information technology security practices of state agencies.

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

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

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

- (1) the State Board for Educator Certification;
- (2) a school district, charter school, private school, regional education service center, commercial transportation company, or education shared service arrangement;
- (3) the Texas Medical Board;
- (4) the Texas School for the Blind and Visually Impaired;
- (5) the Board of Law Examiners;
- (6) the State Bar of Texas;
- (7) a district court regarding a petition for name change under Subchapter B, Chapter 45, Family Code;
- (8) the Texas School for the Deaf;
- (9) the Department of Family and Protective Services;
- (10) the Texas Youth Commission;
- (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 Department of Information Resources but only
24 regarding an employee, applicant for employment, contractor,
25 subcontractor, intern, or volunteer who provides network security
26 services under Chapter 2059 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 identification division of the Federal Bureau of
9 Investigation the criminal history record information maintained
10 by the department or division that relates to a person who is an
11 employee, applicant for employment, contractor, subcontractor,
12 intern, or other volunteer with the Department of Information
13 Resources or with a contractor or subcontractor for the Department
14 of 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:

18 (1) by court order; or

19 (2) with the consent of the person who is the subject
20 of the information.

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

26 (d) The Department of Information Resources may not obtain
27 criminal history record information under this section unless the

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

9 (1) the specific duties of the position;

10 (2) the number of offenses committed by the
11 individual;

12 (3) the nature and seriousness of each offense;

13 (4) the length of time between the offense and the
14 employment decision;

15 (5) the efforts by the individual at rehabilitation;

16 and

17 (6) the accuracy of the information on the
18 individual's employment application.

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

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

24 (1) security assessments or deployments relating to
25 information resources technology;

26 (2) network security information as described by
27 Section 2059.055(b); or

1 (3) the deployment, or specific occasions for
2 implementation, of security personnel, critical infrastructure, or
3 security devices.

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

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

12 (b) The following information is confidential:

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

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

1 disclosure for purposes of Section 552.007.

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

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

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

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

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

1 the state agency's or state agency contractor's computers, computer
2 programs, computer networks, computer systems, computer software,
3 data processing, or electronically stored information. The summary
4 is available to the public on request.

5 SECTION 6. Section 2054.100(b), Government Code, is amended
6 to read as follows:

7 (b) The plan must describe the agency's current and proposed
8 projects for the biennium, including how the projects will:

9 (1) benefit individuals in this state and benefit the
10 state as a whole;

11 (2) use, to the fullest extent, technology owned or
12 adapted by other state agencies;

13 (3) employ, to the fullest extent, the department's
14 information technology standards, including Internet-based
15 technology standards;

16 (4) expand, to the fullest extent, to serve residents
17 of this state or to serve other state agencies;

18 (5) develop on time and on budget;

19 (6) produce quantifiable returns on investment; and

20 (7) meet any other criteria developed by the
21 department or the quality assurance team.

22 SECTION 7. Subchapter B, Chapter 2059, Government Code, is
23 amended by adding Section 2059.060 to read as follows:

24 Sec. 2059.060. VULNERABILITY TESTING OF NETWORK HARDWARE
25 AND SOFTWARE. (a) The department shall adopt rules requiring, in
26 state agency contracts for network hardware and software, a
27 statement by the vendor certifying that the network hardware or

1 software, as applicable, has undergone independent certification
2 testing for known and relevant vulnerabilities.

3 (b) Rules adopted under Subsection (a) may:

4 (1) provide for vendor exemptions; and

5 (2) establish certification standards for testing
6 network hardware and software for known and relevant
7 vulnerabilities.

8 (c) Unless otherwise provided by rule, the required
9 certification testing must be conducted under maximum load
10 conditions in accordance with published performance claims of a
11 hardware or software manufacturer, as applicable.

12 SECTION 8. (a) The Department of Information Resources
13 shall adopt the rules required by Section 2059.060, Government
14 Code, as added by this Act, not later than September 1, 2010.

15 (b) The change in law made by Section 2059.060, Government
16 Code, as added by this Act, applies only to a contract entered into
17 on or after December 1, 2010.

18 SECTION 9. This Act takes effect September 1, 2009.

President of the Senate

Speaker of the House

I certify that H.B. No. 1830 was passed by the House on April 2, 2009, by the following vote: Yeas 144, Nays 0, 1 present, not voting; and that the House concurred in Senate amendments to H.B. No. 1830 on May 14, 2009, by the following vote: Yeas 142, Nays 0, 1 present, not voting.

Chief Clerk of the House

I certify that H.B. No. 1830 was passed by the Senate, with amendments, on May 7, 2009, by the following vote: Yeas 31, Nays 0.

Secretary of the Senate

APPROVED: _____

Date

Governor