

1-1 By: Corte (Senate Sponsor - Ellis) H.B. No. 2233
1-2 (In the Senate - Received from the House April 23, 2007;
1-3 May 1, 2007, read first time and referred to Committee on
1-4 Government Organization; May 19, 2007, reported adversely, with
1-5 favorable Committee Substitute by the following vote: Yeas 4,
1-6 Nays 0; May 19, 2007, sent to printer.)

1-7 COMMITTEE SUBSTITUTE FOR H.B. No. 2233 By: Ellis

1-8 A BILL TO BE ENTITLED
1-9 AN ACT

1-10 relating to information technology security practices of state
1-11 agencies.

1-12 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

1-13 SECTION 1. Subchapter F, Chapter 411, Government Code, is
1-14 amended by adding Section 411.1406 to read as follows:

1-15 Sec. 411.1406. ACCESS TO CRIMINAL HISTORY RECORD
1-16 INFORMATION: DEPARTMENT OF INFORMATION RESOURCES. (a) The
1-17 Department of Information Resources is entitled to obtain from the
1-18 department or another appropriate law enforcement agency the
1-19 criminal history record information maintained by the department or
1-20 other law enforcement agency that relates to:

1-21 (1) a person who is an applicant for employment with
1-22 the Department of Information Resources;

1-23 (2) a person who may perform services for the
1-24 Department of Information Resources; or

1-25 (3) a person who is an employee or subcontractor, or an
1-26 applicant to be an employee or subcontractor, of a contractor that
1-27 provides services to the Department of Information Resources.

1-28 (b) Criminal history record information obtained by the
1-29 Department of Information Resources under Subsection (a) may be
1-30 used only to evaluate:

1-31 (1) an applicant for employment with the Department of
1-32 Information Resources;

1-33 (2) a person who may perform services for the
1-34 Department of Information Resources; or

1-35 (3) a person who is an employee or subcontractor, or an
1-36 applicant to be an employee or subcontractor, of a contractor that
1-37 provides services to the Department of Information Resources.

1-38 (c) Criminal history record information obtained by the
1-39 Department of Information Resources under this section may not be
1-40 released or disclosed to any person or agency except on court order
1-41 or with the consent of the person who is the subject of the
1-42 information.

1-43 (d) The Department of Information Resources shall destroy
1-44 the criminal history record information obtained by this section
1-45 after the information is used for the purposes authorized by this
1-46 section.

1-47 SECTION 2. Subchapter D, Chapter 551, Government Code, is
1-48 amended by adding Section 551.089 to read as follows:

1-49 Sec. 551.089. DEPARTMENT OF INFORMATION RESOURCES. This
1-50 chapter does not require the governing board of the Department of
1-51 Information Resources to conduct an open meeting to deliberate:

1-52 (1) security assessments or deployments relating to
1-53 information resources technology;

1-54 (2) network security information as described by
1-55 Section 2059.055(b); or

1-56 (3) the deployment, or specific occasions for
1-57 implementation, of security personnel, critical infrastructure, or
1-58 security devices.

1-59 SECTION 3. Section 552.139, Government Code, is amended to
1-60 read as follows:

1-61 Sec. 552.139. EXCEPTION: GOVERNMENT INFORMATION RELATED TO
1-62 SECURITY OR INFRASTRUCTURE ISSUES FOR COMPUTERS. (a) Information
1-63 is excepted from the requirements of Section 552.021 if it is

2-1 information that relates to computer network security, to
 2-2 restricted information under Section 2059.055, or to the design,
 2-3 operation, or defense of a computer network.

2-4 (b) The following information is confidential:

2-5 (1) a computer network vulnerability report; and
 2-6 (2) any other assessment of the extent to which data
 2-7 processing operations, a computer, ~~or~~ a computer program,
 2-8 network, system, or system interface, or software of a governmental
 2-9 body or of a contractor of a governmental body is vulnerable to
 2-10 unauthorized access or harm, including an assessment of the extent
 2-11 to which the governmental body's or contractor's electronically
 2-12 stored information containing sensitive or critical information is
 2-13 vulnerable to alteration, damage, ~~or~~ erasure, or inappropriate
 2-14 use.

2-15 (c) Notwithstanding the confidential nature of the
 2-16 information described in this section, the information may be
 2-17 disclosed to a bidder if the governmental body determines that
 2-18 providing the information is necessary for the bidder to provide an
 2-19 accurate bid. A disclosure under this subsection is not a voluntary
 2-20 disclosure for purposes of Section 552.007.

2-21 SECTION 4. Subchapter C, Chapter 2054, Government Code, is
 2-22 amended by adding Sections 2054.064 and 2054.065 to read as
 2-23 follows:

2-24 Sec. 2054.064. VULNERABILITY STANDARDS. (a) The
 2-25 department by rule shall establish standards for protection of
 2-26 computers, computer programs, computer networks, computer systems,
 2-27 interfaces to computer systems, computer software, and data
 2-28 processing of state agencies and of contractors of state agencies
 2-29 from internal and external unauthorized access or harm, including
 2-30 alteration, damage, theft, erasure, or inappropriate use of
 2-31 electronically stored information.

2-32 (b) The department by rule shall establish standards for
 2-33 performance of risk assessments by state agencies, including
 2-34 assessments of information resources that store or transmit
 2-35 sensitive or critical information, and development of
 2-36 vulnerability reports to be used in complying with rules adopted
 2-37 under Subsection (a).

2-38 (c) The department by rule shall establish standards for the
 2-39 implementation by state agencies of physical security and disaster
 2-40 recovery requirements for computer systems that maintain sensitive
 2-41 or critical information. The executive director may establish
 2-42 alternate standards or exceptions to the standards adopted under
 2-43 this subsection for certain classes of servers or mainframes.

2-44 Sec. 2054.065. VULNERABILITY ASSESSMENTS. (a) The
 2-45 department shall annually rank state agencies in order of priority
 2-46 for vulnerability assessments based on a review of agency risks,
 2-47 the need for updated agency information, and the availability of
 2-48 resources. Each agency identified as a priority by the department
 2-49 shall be notified and shall use the external network vulnerability
 2-50 assessment security services provided through the department.

2-51 (b) The department shall annually conduct a statewide
 2-52 assessment of information technology security resources and
 2-53 practices of state agencies, including an analysis of vulnerability
 2-54 reports provided to the department under Section 2054.077. Not
 2-55 later than December 31 of each year, the department shall submit a
 2-56 report on the results of the department's assessment to the
 2-57 governor, the lieutenant governor, the speaker of the house of
 2-58 representatives, and the state auditor's office. The assessment
 2-59 and report prepared under this section are confidential.

2-60 (c) In addition to other protections that may be available
 2-61 under law, a vulnerability report and supporting documentation
 2-62 provided to the state auditor's office under Subsection (b) is
 2-63 incorporated into the risk assessment process of the state auditor.
 2-64 A vulnerability report provided to the state auditor under
 2-65 Subsection (b) is exempt from disclosure under Section 552.116.

2-66 SECTION 5. Sections 2054.077(b), (d), and (e), Government
 2-67 Code, are amended to read as follows:

2-68 (b) In addition to any assessment required under Section
 2-69 2054.065, the [The] information resources manager of a state agency

3-1 may prepare or have prepared a report, including an executive
3-2 summary of the findings of the report, assessing the extent to which
3-3 a computer, a computer program, a computer network, a computer
3-4 system, an interface to a computer system, computer software, or
3-5 data processing of the agency or of a contractor of the agency is
3-6 vulnerable to unauthorized access or harm, including the extent to
3-7 which the agency's or contractor's electronically stored
3-8 information containing sensitive or critical information is
3-9 vulnerable to alteration, damage, ~~or~~ erasure, or inappropriate
3-10 use.

3-11 (d) The ~~[On request, the]~~ information resources manager
3-12 shall provide an electronic ~~[a]~~ copy of the vulnerability report on
3-13 its completion to:

- 3-14 (1) the department;
- 3-15 (2) the state auditor; ~~[and]~~
- 3-16 (3) the agency's executive director; and
- 3-17 (4) any other information technology security
3-18 oversight group specifically authorized by the legislature to
3-19 receive the report.

3-20 (e) Separate from the executive summary described by
3-21 Subsection (b), a [A] state agency whose information resources
3-22 manager has prepared or has had prepared a vulnerability report
3-23 shall prepare a summary of the report that does not contain any
3-24 information the release of which might compromise the security of
3-25 the state agency's or state agency contractor's computers, computer
3-26 programs, computer networks, computer systems, computer software,
3-27 data processing, or electronically stored information. The summary
3-28 is available to the public on request.

3-29 SECTION 6. Subchapter F, Chapter 2054, Government Code, is
3-30 amended by adding Section 2054.114 to read as follows:

3-31 Sec. 2054.114. COMPUTER INCIDENTS. (a) In this section, a
3-32 "computer incident" means a violation or imminent threat of
3-33 violation of computer security policies, acceptable use policies,
3-34 or standard computer security practices that occurs within state
3-35 government.

3-36 (b) A state agency shall promptly investigate, document,
3-37 and report to the department each suspected or confirmed computer
3-38 incident that:

- 3-39 (1) involves sensitive, confidential, or personally
3-40 identifiable information;
- 3-41 (2) is critical in nature; or
- 3-42 (3) could be propagated to other state systems.

3-43 (c) If criminal activity is suspected regarding a computer
3-44 incident, the state agency shall contact the department and
3-45 appropriate law enforcement and investigative authorities
3-46 immediately.

3-47 (d) The department shall adopt rules to implement this
3-48 section.

3-49 SECTION 7. Section 2059.001, Government Code, is amended by
3-50 adding Subdivision (1-a) to read as follows:

3-51 (1-a) "Consolidated state network" means the
3-52 consolidated telecommunications system defined by Section
3-53 2170.001.

3-54 SECTION 8. The Department of Information Resources shall
3-55 adopt rules required by Section 2054.064, Government Code, as added
3-56 by this Act, not later than January 1, 2008.

3-57 SECTION 9. This Act takes effect September 1, 2007.

3-58 * * * * *