By: Corte H.B. No. 2233

Substitute the following for H.B. No. 2233:

By: Corte C.S.H.B. No. 2233

A BILL TO BE ENTITLED

AN ACT

relating to information technology security practices of state agencies.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SECTION 3. Section 552.139, Government Code, is amended to

read as follows:

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

(b) The following information is confidential:

(1) a computer network vulnerability report; and

(2) any other assessment of the extent to which data processing operations, a computer, [~~or~~] a computer program, network, system, or system interface, or software of a governmental body or of a contractor of a governmental body is vulnerable to unauthorized access or harm, including an assessment of the extent to which the governmental body's or contractor's electronically stored information containing sensitive or critical information is vulnerable to alteration, damage, [~~or~~] erasure, or inappropriate use.

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

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

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

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

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

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

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

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

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

(b) In addition to any assessment required under Section 2054.065, the [~~The~~] information resources manager of a state agency may prepare or have prepared a report, including an executive summary of the findings of the report, assessing the extent to which a computer, a computer program, a computer network, a computer system, an interface to a computer system, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information containing sensitive or critical information is

vulnerable to alteration, damage, [~~or~~] erasure, or inappropriate use.

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

(1) the department;

(2) the state auditor; [~~and~~]

(3) the agency's executive director; and

(4) any other information technology security oversight group specifically authorized by the legislature to receive the report.

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

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

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

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

(1) involves sensitive, confidential, or personally identifiable information;

(2) is critical in nature; or

(3) could be propagated to other state systems.

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

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

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

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

SECTION 9. This Act takes effect September 1, 2007.