BILL ANALYSIS

Senate Research Center
81R29254 E

C.S.H.B. 1830
By: Corte, Edwards (Ellis)
Government Organization
5/1/2009
Committee Report (Substituted)

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Current law allows the Department of Information Resources (DIR) to conduct criminal history background checks on potential and current employees who have access to information technology, but not other sensitive information DIR deals with. Current law also requires all meetings of the DIR board to be open to the public and allows the vulnerability report to include the extent to which information is vulnerable to alteration, damage, or erasure.

C.S.H.B. 1830 amends current law relating to information technology security practices of state agencies.

RULEMAKING AUTHORITY

Rulemaking authority is expressly granted to the Department of Information Resources in SECTION 7 (Section 2059.060, Government Code) of this bill.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends 411.081(i), Government Code, to authorize a criminal justice agency to disclose criminal history record information that is the subject of an order of nondisclosure to certain noncriminal justice agencies or entities only, including the Department of Information Resources (DIR) but only regarding an employee, applicant for employment, contractor, subcontractor, intern, or volunteer who provides network security services under Chapter 2059 (Texas Computer Network Security System), to DIR or a contractor or subcontractor of DIR. Makes a nonsubstantive change.

SECTION 2. Amends Subchapter F, Chapter 411, Government Code, by adding Section 411.1404, as follows:

> Sec. 411.1404. ACCESS TO CRIMINAL HISTORY RECORD INFORMATION: DEPARTMENT OF INFORMATION RESOURCES. (a) Entitles DIR to obtain from DIR or the identification division of the Federal Bureau of Investigation the criminal history record information maintained by DIR that relates to a person who is an employee, applicant for employment, contractor, subcontractor, intern, or volunteer with DIR or with a contractor or subcontractor for DIR.
>
> (b) Prohibits criminal history record information obtained by DIR under this section from being released or disclosed except by court order or with the consent of the person who is the subject of the information.
>
> (c) Requires DIR to destroy criminal history record information obtained under this section that relates to a person after the information is used to make an employment decision or to take a personnel action relating to the person who is the subject of the information.
>
> (d) Prohibits DIR from obtaining criminal history record information under this section unless DIR first adopts policies and procedures that provide that evidence of a criminal conviction or other relevant information obtained from the criminal history record information does not automatically disqualify an individual from employment. Requires that the policies and procedures adopted under this subsection provide that the hiring official will determine, on a case-by-case basis,

whether the individual is qualified for employment based on factors that include the specific duties of the position; the number of offenses committed by the individual; the nature and seriousness of each offense; the length of time between the offense and the employment decision; the efforts by the individual at rehabilitation; and the accuracy of the information on the individual's employment application.

SECTION 3. Amends Subchapter D, Chapter 551, Government Code, by adding Section 551.089, as follows:

Sec. 551.089. DEPARTMENT OF INFORMATION RESOURCES. Provides that this chapter does not require the governing board of DIR to conduct an open meeting to deliberate security assessments or deployments relating to information resources technology; network security information as described by Section 2059.055(b) (relating to the confidentiality of network security information); or the deployment, or specific occasions for implementation, of security personnel, critical infrastructure, or security devices.

SECTION 4. Amends Section 552.139, Government Code, as follows:

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

(b) Provides that the following is confidential: a computer network vulnerability report; and any other assessment of the extent to which data processing operations, a computer, 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, erasure, or inappropriate use. Makes nonsubstantive changes.

(c) Authorizes the information, notwithstanding the confidential nature of the information described in this section, to be disclosed to a bidder if the governmental body determines that providing the information is necessary for the bidder to provide an accurate bid. Provides that a disclosure under this subsection is not a voluntary disclosure for purposes of Section 552.007 (Voluntary Disclosure of Certain Information When Disclosure Not Required).

SECTION 5. Amends Sections 2054.077(b), (d), and (e), Government Code, as follows:

(b) Authorizes the information resources manager of a state agency to 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 is vulnerable to alteration, damage, erasure, or inappropriate use. Makes a nonsubstantive change.

(d) Requires the information resources manager to provide, rather than provide on request, an electronic copy of the vulnerability report on its completion to certain entities, including the agency's executive director. Makes nonsubstantive changes.

(e) Requires a state agency whose information resources manager has prepared or has had prepared a vulnerability report, separate from the executive summary described by Subsection (b), to 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. Provides that the summary is available to the public on request.

SECTION 6. Amends Section 2054.100(b), Government Code, to require that the biennial operating plan describe the state agency's current and proposed projects for the biennium, including how the projects will address certain matters, including using, to the fullest extent, technology owned or adapted by other state agencies, including closed loop event management technology that secures, logs, and provides audit management of baseboard management controllers and consoles of cyber assets.

SECTION 7. Amends Subchapter B, Chapter 2059, Government Code, by adding Section 2059.060, as follows:

Sec. 2059.060. VULNERABILITY TESTING OF NETWORK HARDWARE AND SOFTWARE. (a) Requires DIR to adopt rules requiring, in state agency contracts for network hardware and software, a statement by the vendor certifying that the network hardware or software, as applicable, has undergone independent certification testing for known and relevant vulnerabilities.

(b) Authorizes rules adopted under Subsection (a) to provide for vendor exemptions and establish certification standards for testing network hardware and software for known and relevant vulnerabilities.

(c) Requires that the required certification testing, unless otherwise provided by rule, be conducted under maximum load conditions in accordance with published performance claims of a hardware or software manufacturer, as applicable.

SECTION 8. (a) Requires DIR to adopt the rules required by Section 2059.060, Government Code, as added by this Act, not later than September 1, 2010.

(b) Makes application of Section 2059.060, Government Code, as added by this Act, prospective to December 1, 2010.

SECTION 9. Effective date: September 1, 2009.