

BILL ANALYSIS

C.S.H.B. 1830
By: Corte
Defense & Veterans' Affairs
Committee Report (Substituted)

BACKGROUND AND PURPOSE

The security of government technology, which includes both the physical and logical security of the state's data systems and networks, is a shared and vital responsibility that requires continuous, coordinated, and focused efforts. For many business and government organizations, major computer security incidents with financial and operational impacts have become common occurrences. To cope with ongoing threats, the Department of Information Resources (DIR) and other state agencies must collaborate to preserve the confidentiality, integrity, and availability of the state's networks. While DIR has the authority to conduct criminal history background checks on potential and current employees and contractors, this authority is limited to technical staff. Studies conducted by the Identity Theft Resource Center show that 20 to 30 percent of insider misconduct originates with employees who have prior criminal records, and most of these employees do not have advanced technical skills or privileged technology access.

C.S.H.B. 1830 authorizes criminal history background checks for all potential and current employees and contractors and requires greater communication within agencies and with DIR regarding assessments of network vulnerabilities.

RULEMAKING AUTHORITY

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

ANALYSIS

C.S.H.B. 1830 amends the Government Code to include the Department of Information Resources, among the agencies to which a criminal justice agency is authorized to disclose criminal history record information that is the subject of an order of nondisclosure for certain persons as provided by the bill. The bill entitles the department to obtain from the Department of Public Safety (DPS) or the identification division of the Federal Bureau of Investigation the criminal history record information maintained by DPS or the division that relates to a person who is an employee, applicant for employment, contractor, subcontractor, intern, or other volunteer with the department or with a contractor or subcontractor for the department and provides network security services under provisions relating to the Texas computer network security system. The bill prohibits criminal history record information obtained by the department from being released or disclosed except by court order or with the consent of the person who is the subject of the information. The bill requires the department to destroy the criminal history record information 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.

C.S.H.B. 1830 prohibits the department from obtaining criminal history record information unless the department 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. The bill requires

the adopted policies and procedures to 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.

C.S.H.B. 1830 establishes that the open meetings law does not require the governing board of the department to conduct an open meeting to deliberate: security assessments or deployments relating to information resources technology; confidential network security information; or the deployment, or specific occasions for implementation, of security personnel, critical infrastructure, or security devices. The bill exempts restricted information as described under provisions relating to the Texas computer network security system from provisions requiring the information to be available to the public during normal business hours. The bill makes any vulnerability assessment of a governmental body's or contractor of a governmental body's system interface confidential information, and specifies that the assessment of a contractor's or governmental body's electronically stored information includes the extent to which the information is vulnerable to inappropriate use, in addition to alteration, damage, or erasure. The bill authorizes the information 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 and establishes that such a disclosure is not a voluntary disclosure for purposes of a provision relating to voluntary disclosure of public information.

C.S.H.B. 1830 authorizes the information resources manager of a state agency to include an executive summary of findings in a vulnerability report and an assessment to the extent to which a computer system interface is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to inappropriate use, in addition to alteration, damage, or erasure. The bill specifies that the vulnerability report is required to be provided to certain recipients on its completion, rather than on request, and that the copy provided be an electronic copy. The bill includes the agency's executive director as a recipient of the vulnerability report.

EFFECTIVE DATE

September 1, 2009.

COMPARISON OF ORIGINAL AND SUBSTITUTE

C.S.H.B. 1830 differs from the original by adding a condition that was not in the original on the authority of a criminal justice agency to disclose information to the Department of Information Resources to provide that the disclosure is subject to the provision in the substitute entitling the department to obtain certain criminal history record information. The substitute differs from the original by specifying that the department is entitled to obtain criminal history record information that relates to certain persons from the identification division of the Federal Bureau of Investigation, rather than another appropriate law enforcement agency as in the original. The substitute differs from the original by adding a contractor, subcontractor, intern, or other volunteer with the department or with a contractor or subcontractor for the department to those persons whose criminal history record information the department is entitled to access and by adding the criteria that the person for whom the department has a right to information is a person who provides network security services under the Texas computer network security system. The substitute differs from the original by removing a person described as a person who may perform services for the department from those persons whose criminal history record information the department is entitled to access.

C.S.H.B. 1830 removes a provision from the original that listed the purposes for which the criminal history record information obtained by the department could be used including

evaluating an employee or applicant for employment with the department, a person who may perform services for the department, or 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.

C.S.H.B 1830 differs from the original by clarifying that the department is required to destroy the criminal history record information 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, rather than after the information is used for the purposes of the provision. The substitute adds provisions not in the original to prohibit the department from obtaining criminal history record information unless the department first adopts certain policies and procedures.

C.S.H.B. 1830 differs from the original by removing language in the original that described the type of electronically stored information that must be discussed in the executive summary as information containing sensitive or critical information.