BILL ANALYSIS

C.S.H.B. 2233
By: Corte, Frank
Defense Affairs & State-Federal Relations
Committee Report (Substituted)

BACKGROUND AND PURPOSE

The security of information and communications technology resources is a shared responsibility that requires continuous, coordinated, and focused efforts. Texas state government's infrastructure is a critical resource that needs to remain functional and secure. Over 19 million incidents related to information technology security were detected and reported to the Department of Information Resources (DIR) by state entities during FY 2006. As a result of effective detection and antivirus measures, the scope of the actual infections was minimized. Still, state entities expended an estimated 8,400 hours in remediation efforts, at an estimated cost of approximately $1.9 million. Improvements to the state's information and network security programs are needed to reduce the vulnerability of the state's infrastructure to attacks, which are increasing in number, complexity, and severity. To cope with these and other information security attacks, the Department of Information Resources (DIR) and state agencies need to work together to identify and assess vulnerabilities and remediate potential risks to keep the state's networks open, operational and secure.

CSHB 2233 seeks to address these efforts by requiring regular risk assessments, vulnerability testing, and timely and more complete reporting of computer security incidents.

RULEMAKING AUTHORITY

It is the committee's opinion that rulemaking authority is expressly granted to the Department of Information Resources in SECTION 4 (Section 2054.064, Government Code) of this bill.

ANALYSIS

CSHB 2233 adds Section 411.1406, Government Code, to allow DIR to access criminal history record information for employees, job applicants, and subcontractors. This information may be used only to evaluate those persons, and may not be released or disclosed except by court order or with that person's consent, and must be destroyed after the information is used for the purpose authorized in the bill.

CSHB 2233 adds Section 551.089, Government Code, to allow DIR's governing board to meet in executive session to deliberate security assessments or deployments relating to information resources technology, certain network security information, or the deployment or specific occasions for implementation, of security personnel, critical infrastructure, or security devices. It amends Section 552.139, Government Code, to exempt information about an agency's computer infrastructure from the open records act and to allow the disclosure of that information to a bidder if the information is needed for an accurate bid.

CSHB 2233 adds Sections 2054.064 and 2054.065, Government Code, to direct DIR to adopt rules to establish standards to ensure the security of agencies' computers, computer programs, networks and related systems, software, and data processing and of contractors of state agencies from internal and external unauthorized access or harm. Further, it directs DIR, by rule, to establish standards for performance of risk assessments by state agencies and, by rule, to establish standards for the implementation by state agencies of physical security and disaster recovery requirements for computer systems that maintain sensitive or critical information. It requires DIR to annually rank state agencies in order of priority for vulnerability assessments and to conduct an annual statewide assessment of the information technology security resources and practices of state agencies, including an analysis of vulnerability reports of individual state agencies, and to report annually on the results of the department's assessment to the governor, lieutenant governor, speaker and the state auditor. The assessment and report under this section are confidential and not subject to open records.

CSHB 2233 amends Section 2054.077(b), (d) and (e), Government Code, to require that, if an agency prepares a vulnerability assessment report, in addition to any assessment required under Section 2054.065, the report, including an executive summary of the findings of the report, must be submitted electronically to the agency's executive director, among others. Separate from the executive summary, an agency that prepares a vulnerability report shall prepare a summary of that report, that does not contain confidential information, to be made available to the public on request.

CSHB 2233 adds section 2054.114, Government Code, to require state agencies to investigate, document and report certain computer incidents, as defined by the bill, to DIR and to law enforcement authorities if criminal activity is suspected. Further, CSHB 2233 amends Section 2059.001, Government Code, to add "consolidated state network" to the definition of "consolidated telecommunications system." It directs DIR to adopt required rules by January 1, 2008.

EFFECTIVE DATE

September 1, 2007.

COMPARISON OF ORIGINAL TO SUBSTITUTE

The substitute amends SECTION 5 of the bill to clarify that the information manager shall provide an electronic copy of the vulnerability report to the department and the agency's executive director, among others, not just on request. It amends SECTION 6 of the bill to clarify which computer incidents are to be investigated, documented and reported. And, finally, the substitute amends SECTION 8, by changing the date by which the department shall adopt rules from October 1, 2007 to January 1, 2008.