BILL ANALYSIS

Senate Research Center
80R12338 TAD-D

C.S.S.B. 1036
By: Ellis
Government Organization
4/4/2007
Committee Report (Substituted)

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

The security of information and communications technology resources is a shared responsibility that requires continuous, coordinated, and focused efforts. The state government's infrastructure is a critical resource that must remain functional and secure at all times. For many business and governmental entities, major computer security incidents with significant financial and operational impacts are becoming common occurrences. 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.

Over 19 millions incidents related to information technology security were detected and reported to the Department of Information Resources (DIR) by state entities during fiscal year (FY) 2006. As a result of effective detection and antivirus measures, reported actual infections were limited to 22,030 desktop computers and servers. While the scope of the actual infections was minimized, state entities expended more than 8,400 hours in remediation efforts, at an estimated cost of approximately $1.9 million.

To cope with these and other information security attacks, DIR and state agencies must work together to constantly identify and assess vulnerabilities and remediate potential risks to keep the state's networks open, operational, and secure. These efforts include regular assessments, vulnerability testing, proactive remediation, and more timely and complete reporting of computer security incidents.

C.S.S.B. 1036 requires DIR to conduct vulnerability assessments for state agencies based on risk assessment and requires DIR to adopt rules to ensure the protection of computer systems and the security and disaster recovery capability of the computer systems of state agencies. This bill requires DIR to produce an annual confidential report on the information technology resources and practices of state agencies, and requires state agencies to report computer incidents to DIR. This bill authorizes DIR to conduct closed meetings for certain security-related deliberations.

RULEMAKING AUTHORITY

Rulemaking authority is expressly granted to the Department of Information Resources in SECTION 4 (Section 2054.064, Government Code) of this bill.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Subchapter F, Chapter 411, Government Code, by adding Section 411.1406, as follows:

> Sec. 411.1406. ACCESS TO CRIMINAL HISTORY RECORD INFORMATION: DEPARTMENT OF INFORMATION RESOURCES. (a) Entitles the Department of Information Resources (DIR) to obtain from the Department of Public Safety (DPS) the criminal history record information (information) maintained by DPS or another law enforcement agency that relates to certain persons.
>
> (b) Requires that the information obtained by DIR to be used only to evaluate certain persons.

(c) Prohibits the information obtained by DIR from being 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) Requires DIR to destroy the information after it is used for the purposes authorized by this section.

SECTION 2. Amends Subchapter D, Chapter 551, Government Code, by adding Section 551.089, provide that this chapter (Open Meetings) does not require the governing board of DIR to conduct open meetings to deliberate certain issues.

SECTION 3. 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) Exempts from the requirements of Section 552.021 (Availability of Public Information) information relating to computer network security, restricted information under Section 2059.055 (Texas Computer Network Security System), or the design, operation, or defense of a computer network.

(b) Provides that certain information is confidential.

(c) Authorizes the confidential 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 said disclosure is not a voluntary disclosure for purposes of Section 552.007 (Voluntary Disclosure of Certain Information When Disclosure is not Required).

SECTION 4. Amends Subchapter C, Chapter 2054, Government Code, by adding Sections 5054.064 and 6054.065, as follows:

Sec. 2054.064. VULNERABILITY STANDARDS. (a) Requires DIR by rule to establish standards for the protection of certain information from internal and external unauthorized access or harm.

(b) Requires DIR by rule to establish standards for performance of risk assessments by state agencies, including of information resources, and the development of vulnerability reports to be used in complying with those adopted rules.

(c) Requires DIR by rule to establish standards for the implementation of physical security and disaster requirements for computer systems that maintain sensitive or critical information. Authorizes the executive director of DIR to establish alternate standards or exceptions to the adopted standards under this subsection for certain classes of servers or mainframes.

Sec. 2054.065. VULNERABILITY ASSESSMENTS. (a) Requires DIR to annually rank state agencies in order of priority for vulnerability assessments based on certain criteria. Requires each agency identified as a priority to be notified and to use the external network vulnerability assessment security services provided through DIR.

(b) Requires DIR to annually conduct a statewide assessment of information technology security resources and practices. Requires DIR to submit a report on the results of the assessment to certain persons not later than December 31 of each year. Provides that the assessment reports are confidential.

(c) Provides that a vulnerability report and supporting documentation provided to the state auditor under Subsection (b) is incorporated into the risk assessment process thereof and is exempt from disclosure under Section 552.116 (Exception: Audit Working Papers).

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 vulnerability report, including an executive summary, assessing the extent to which certain programs or systems are vulnerable to unauthorized access or harm, including the extent to which electronically stored information containing sensitive or critical information is vulnerable to alteration, damage, erasure, or inappropriate use.

(d) Requires the information resources manager to provide an electronic copy of the vulnerability report on completion to certain persons, including the agency's executive director.

(e) Provides that the required summary under this subsection is separate from the executive summary described by Subsection (b).

SECTION 6. Amends Subchapter F, Chapter 2054, Government Code, by adding Section 2054.114, as follows:

Sec. 2054.114. COMPUTER INCIDENTS. (a) Defines "computer incident."

(b) Requires state agencies to promptly investigate, document, and report to DIR each suspected or confirmed computer incident that involves sensitive, confidential, or personally identifiable information, is critical in nature, or could be propagated to other state systems.

(c) Requires the state agency to contact DIR, appropriate law enforcement, and investigative authorities immediately if criminal activity is suspected regarding a computer incident.

SECTION 7. Amends Section 2059.001, Government Code, by adding Subdivision (1-a), to define "consolidated state network."

SECTION 8. Requires DIR to adopt rules required by Section 2054.064 not later than January 1, 2008.

SECTION 9. Effective date: September 1, 2007.