BILL ANALYSIS

C.S.H.B. 3112
By: Corte
Defense Affairs & State-Federal Relations
Committee Report (Substituted)

BACKGROUND AND PURPOSE

The security of State computer networks is currently handled by each agency on an independent basis. As computer needs arise, agencies with resources to fill these needs often find solutions, while agencies with limited resources are often forced to choose between accessibility and security. This fragmented network security approach can lead to overlapping and redundant state assets on one hand which cost more money than necessary, and a lack of security features on the other hand where monetary resources are lacking. A recent report by the Department of Information Resources recommends that the State must develop a shared statewide technology infrastructure to support increasing demands on agency operations. In response, the DIR is embarking on a major effort to consolidate the computer networks of most, or all State agencies over time. Combined with the Data Center consolidation initiative, this will enable consolidation of facilities, mainframes, data storage management and other common computer needs, saving the State millions of dollars annually.

As part of this overall consolidation effort, CSHB 3112 provides for a system of shared computer security throughout the State agencies that are consolidated. This will provide for a shared security architecture that can be used by all agencies to provide expert cyber security services. The DIR is required in the bill to provide network security services to state agencies, and may provide these services to other entities by agreement. As the Department of Information Resources consolidates the computer networks, they shall provide the security as part of the consolidation. The bill creates a Network Security Center into which the State can eventually consolidate all state network security. This centralized Network Security Center would employ computer security experts that will monitor all participating agency networks 24 hours a day, seven days a week. The bill sets out some specific services that are to be provided by the Center. The bill also requires DIR to set up a payment for services billing system to each State agency, or other entity using the services.

RULEMAKING AUTHORITY

It is the committee's opinion that rulemaking authority is expressly granted to the Department of Information Resources in SECTION 1 (Subchapter B, Section 2059.052, Government Code) in this bill.

ANALYSIS

CSHB 3112 sets out that the Department of Information Resources (DIR) is responsible for providing computer network security services from external security threats to state agencies and other entities, by agreement. The bill restricts specific network security information to responsible officials, law enforcement, state auditor's office or designated agency or elected officials.

The DIR is required to submit a biennial report on the status and accomplishments of the consolidated network security system provided.

The bill allows the DIR to provide network security services to other entities, districts, agencies and organizations by agreements made by the Department and the entity.

The bill establishes the Network Security Center (NSC) for the DIR to provide network security services to state agencies. The DIR is required to provide security services when they consolidate the overall computer network. State agencies are required to use the network security services to the fullest extent possible and the bill prohibits certain purchases of security services unless the DIR determines that the requirement cannot be met at a comparable cost through the Center.

The bill requires that the Center be located at a location that has an existing secure and restricted facility, cyber-security infrastructure, an available trained workforce and supportive educational capabilities. Local law enforcement or security agencies shall monitor security alarms at the center.

Section 2059.104 of the bill sets out specific managed security services that the DIR is to provide through the Center, to include centralized real-time 24-hour continuous network security monitoring, among other duties.

CSHB 3112 requires the Department to adopt security guidelines and procedures to ensure efficient operation of the center with a maximum return on investment for the State.

The bill permits the DIR to contract with a private vendor to build and operate the Center and act as an authorized agent to acquire, install, integrate, maintain, configure and monitor the network security services and infrastructure elements. The bill sets out certain requirements of the vendor.

Section 2059.151 of the bill requires the Department to develop a system of billings and charges for network security services provided that allocates the total state cost to each state agency, or other entity served by the system based on proportionate usage.

The bill also allows the department to apply for and use grants offered by any federal agency, or other source.

EFFECTIVE DATE

This Act takes effect September 1, 2005.

COMPARISON OF THE ORIGINAL TO THE SUBSTITUTE

Section 2059.054 is amended to allow the State Auditor's office the ability to receive certain restricted security information.

Section 2059.056 is changed in the Substitute to specify who is to receive the biennial report and includes the State Auditor's Office to the list.

Section 2059.103 (d) is changed in the Substitute to ensure the state Auditor's ability to access and audit the Center

Section 2059.104 of the Original bill is changed to make certain Center services optional.

Section 2059.104 (b) of the Original bill is stricken in the Substitute.