BILL ANALYSIS

Senate Research Center

H.B. 3112
By: Corte (Wentworth)
Government Organization
5/18/2005
Engrossed

AUTHOR'S/SPONSOR'S STATEMENT OF INTENT

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 (department) recommends that the State must develop a shared statewide technology infrastructure to support increasing demands on agency operations. In response, the department 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, H.B. 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 department 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 consolidates the computer networks, they shall provide the security as part of the consolidation. H.B. 3112 creates a Network Security Center (center) into which the state can eventually consolidate all state network security. This centralized center would employ computer security experts that will monitor all participating agency networks 24 hours a day, seven days a week. H.B. 3112 sets out specific services that are to be provided by the center. H.B. 3112 also requires the department to set up a payment for services billing system to each State agency, or other entity using the services.

RULEMAKING AUTHORITY

Rulemaking authority is expressly granted to the Department of Information Resources in SECTION 1 (Section 2059.052, Government Code) of this bill.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Subtitle B, Title 10, Government Code, by adding Chapter 2059, as follows:

CHAPTER 2059. TEXAS COMPUTER NETWORK SECURITY SYSTEM

SUBCHAPTER A. GENERAL PROVISIONS

Sec.2059.001. DEFINITIONS. Defines "center," "department," "network security," and "state agency."

[Reserves Sections 2059.002-2059.050 for expansion.]

SUBCHAPTER B. GENERAL POWERS AND DUTIES

Sec. 2059.051. DEPARTMENT RESPONSIBLE FOR PROVIDING COMPUTER NETWORK SECURITY SERVICES. Requires the Department of Information

Resources (department) to provide network security services to state agencies and other entities by agreement as provided by Section 2059.057.

Sec. 2059.052. RULES. Authorizes the department to adopt rules necessary to implement this chapter.

Sec. 2059.053. OWNERSHIP OR LEASE OF NECESSARY EQUIPMENT. Authorizes the department to purchase in accordance with Chapters 2155 (Purchasing: General Rules And Procedures), 2156 (Purchasing Methods), 2157 (Purchasing: Purchase of Automated Information Systems) And 2158 (Purchasing: Miscellaneous Provisions For Purchase Of Certain Goods And Services), Government Code, any facilities or equipment necessary to provide network security services to state agencies.

Sec. 2059.054. RESTRICTED INFORMATION. Authorizes specific network information about a state agency to be release only to officials responsible for the network, law enforcement, the state auditor's office, and agency or elected officials designated by the department.

Sec. 2059.055. RESPONSIBILITY FOR EXTERNAL AND INTERNAL SECURITY THREATS. Provides that, if the department provides network security services for a state agency or other entity under this chapter, the department is responsible for network security from external threats for that agency or entity. Provides that network security management for that state agency or entity regarding internal threats remains the responsibility of that state agency or entity.

Sec. 2059.056. BIENNIAL REPORT. Requires the department to biennially prepare a report on the department's accomplishment of service objectives and other performance measures under this chapter and the status, including the financial performance, of the consolidated network security system provided through the center. Requires the department to submit the report to the governor, the lieutenant governor, the speaker of the house of representatives, and the state auditor's office.

Sec. 2059.057. AGREEMENT TO PROVIDE NETWORK SECURITY SERVICES TO ENTITIES OTHER THAN STATE AGENCIES. Defines "special district." Authorizes the department, in addition to the department's duty to provide network security services to state agencies under this chapter, by agreement, to provide network security to certain agencies and entities.

Sec. 2059.058. TRANSITION TO THE CENTER. Requires the department to provide network security services for a state agency if the department makes that state agency's network a part of the consolidated state network through the center. Authorizes the department, before the construction and operation of the center, to provide network security services through agreements with entities that provide those services using existing network security centers or operations. Requires the department, if the state agency or entity pays its proportional share of the network security services costs under this chapter, to provide network security services to that state agency or other entity before the department makes the state agency's network a part of the consolidated state network. Provides that this section expires September 1, 2011.

[Reserves Sections 2059.059-2059.100 for expansion.]

SUBCHAPTER C. NETWORK SECURITY CENTER

Sec. 2059.101. NETWORK SECURITY CENTER. Requires the department to establish a network security center to provide security services to state agencies.

Sec. 2059.102. MANAGEMENT AND USE OF NETWORK SECURITY SYSTEM. Requires the department to manage the operation of network security system services for all state agencies at the center. Requires the department to fulfill requirements of each state agency to the extent practicable. Requires the department to protect criminal justice and homeland security networks of this state to the fullest extent possible in accordance

with federal criminal justice and homeland security network standards. Requires all state agencies to use the network security services provided through the center to the fullest extent possible. Prohibits a state agency from purchasing network security services unless the department determines that the agency's requirement for network security services cannot be met at a comparable cost through the center. Requires the department to develop an efficient process for this determination.

Sec. 2059.103. CENTER LOCATION AND PHYSICAL SECURITY. Requires the department to locate the center at a location that has an existing secure and restricted facility, cyber-security infrastructure, available trained workforce, and supportive educational capabilities. Requires the department to control and monitor all entrances and critical areas to prevent unauthorized entry. Requires the department to limit access to authorized individuals. Requires local law enforcement or security agencies to monitor security alarms at the center according to service availability. Requires the department to restrict operational information to personnel at the center, except as provided by Chapter 321 (State Auditor), Government Code.

Sec. 2059.104. CENTER SERVICES AND SUPPORT. Requires the department to provide certain managed security services through the center. Authorizes the department to provide implementation of best-of-breed information security architecture engineering services, including public key infrastructure development, design, engineering, custom software development, and secure web design or certification and accreditation to ensure compliance with the applicable regulatory requirements for cyber-security and information technology risk management, including the use of proprietary tools to automate the assessment and enforcement of compliance.

Sec. 2059.105. NETWORK SECURITY GUIDELINES AND STANDARD OPERATING PROCEDURES. Requires the department to adopt and provide to all state agencies appropriate network security guidelines and standard operating procedures to ensure efficient operation of the center with a maximum return on investment for the state. Requires the department to revise the standard operating procedures as necessary to confirm network security. Requires each state agency to comply with the network security policies, guidelines, and standard operating procedures.

Sec. 2059.106. PRIVATE VENDOR. Authorizes the department 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 security infrastructure elements. Sets forth specific requirements for a private vendor contracted with under this section.

[Reserves Sections 2059.107-2059.150 for expansion.]

SUBCHAPTER D. FINANCIAL PROVISIONS

Sec. 2059.151. PAYMENT FOR SERVICES. Requires the department to develop a system of billings and charges for services provided in operating and administering the network security system that allocates the total state cost to each state agency or other entity served by the system based on proportionate usage.

Sec. 2059.152. REVOLVING FUND ACCOUNT. Requires the comptroller of public accounts to establish in the state treasury a revolving fund account for the administration of this chapter. Requires the account to be used as a depository for money received from state agencies and other entities served under this chapter. Requires receipts attributable to the centralized network security system to be deposited into the account and separately identified within the account. Authorizes the legislature to appropriate money for operating the system directly to the department, in which case the revolving fund account must be used to receive money due from local governmental entities and other agencies to the extent that their money is not subject to legislative appropriation. Requires the department to maintain in the revolving fund account sufficient amounts to pay the liabilities of the center and related network security services.

Sec. 2059.153. GRANTS. Authorizes the department to apply for and use for purposes of this chapter the proceeds from grants offered by any federal agency or other source.

SECTION 2. (a) Defines "department."

(b) Requires the department to study the interoperability of the network security features for user-specific access as provided by this Act. Requires the department, as part of the study, to determine the potential for interoperability of user access technology and identify resulting cost savings and security benefits to Texas. Requires the department to convene the necessary project staff from affected state agencies, as well as appropriate independent technology experts to determine feasibility, cost savings, scalability, and other relevant factors regarding integration of user-specific access features to state computer network systems that will enhance information security.

(c) Requires the department report on the results of the study and include recommendations in the report regarding integration and user-specific access features that will enhance computer network and information security.

(d) Requires the department, not later than December 31, 2006, to file the report with the lieutenant governor, the speaker of the house of representatives, and the chairs of the house and senate committees with primary oversight over the department.

SECTION 3. Effective date: September 1, 2005.