By: Corte (Senate Sponsor - Wentworth) H.B. No. 3112

(In the Senate - Received from the House May 16, 2005; May 17, 2005, read first time and referred to Committee on Government Organization; May 20, 2005, reported favorably, as amended, by the following vote: Yeas 6, Nays 0; May 20, 2005, sent to printer.)

COMMITTEE AMENDMENT NO. 1 By: Eltife

Amend H.B. No. 3112 (House engrossment) as follows:

(1) In Section 1 of the bill, in added Subchapter B, Chapter 2059, Government Code (page 1, between lines 57 and 58), insert a new Section 2059.052 to read as follows:

Sec. 2059.052. SERVICES PROVIDED TO INSTITUTIONS OF HIGHER EDUCATION. The department may provide network security services to an institution of higher education, and may include an institution of higher education in a center, only if and to the extent approved by the Information Technology Council for Higher Education.

(2) Renumber the sections of Subchapter B, Chapter 2059, Government Code, and cross-references to those sections accordingly.

COMMITTEE AMENDMENT NO. 2 By: Eltife

Amend HB 3112 (Engrossed Version) as follows:

On Page 4, beginning on line 3, strike Section 2059.106 (Engrossed version) and substitute the following:

"Sec. 2059.106. PRIVATE VENDOR. The department may 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."

A BILL TO BE ENTITLED
AN ACT

relating to the security of computer networks in state government.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Subtitle B, Title 10, Government Code, is amended by adding Chapter 2059 to read as follows:

CHAPTER 2059. TEXAS COMPUTER NETWORK SECURITY SYSTEM

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 2059.001. DEFINITIONS. In this chapter:

(1) "Center" means the network security center established under this chapter.

(2) "Department" means the Department of Information Resources.

(3) "Network security" means the protection of computer systems and technology assets from unauthorized external intervention or improper use. The term includes detecting, identifying, and countering malicious network activity to prevent the acquisition of information or disruption of information technology operations.

(4) "State agency" has the meaning assigned by Section 2151.002.

[Sections 2059.002-2059.050 reserved for expansion]

SUBCHAPTER B. GENERAL POWERS AND DUTIES

Sec. 2059.051. DEPARTMENT RESPONSIBLE FOR PROVIDING COMPUTER NETWORK SECURITY SERVICES. The department shall provide network security services to:

(1) state agencies; and

(2) other entities by agreement as provided by Section 2059.057.

Sec. 2059.052. RULES. The department may adopt rules necessary to implement this chapter.

Sec. 2059.053. OWNERSHIP OR LEASE OF NECESSARY EQUIPMENT.

The department may purchase in accordance with Chapters 2155, 2156, 2157, and 2158 any facilities or equipment necessary to provide network security services to state agencies.

Sec. 2059.054. RESTRICTED INFORMATION. Specific network security information about a state agency may be released 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. 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. 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. (a) The department shall biennially prepare a report on:

(1) the department's accomplishment of service objectives and other performance measures under this chapter; and

(2) the status, including the financial performance, of the consolidated network security system provided through the center.

(b) The department shall submit the report to:

(1) the governor;

(2) the lieutenant governor;

(3) the speaker of the house of representatives; and

(4) the state auditor's office.

Sec. 2059.057. AGREEMENT TO PROVIDE NETWORK SECURITY SERVICES TO ENTITIES OTHER THAN STATE AGENCIES. (a) In this section, a "special district" means:

(1) a school district;

(2) a hospital district;

(3) a water district; or

(4) a district or special water authority, as defined by Section 49.001, Water Code.

(b) In addition to the department's duty to provide network security services to state agencies under this chapter, the department by agreement may provide network security to:

(1) each house of the legislature;

(2) an agency that is not a state agency, including a legislative agency;

(3) a political subdivision of this state, including a county, municipality, or special district; and

(4) an independent organization, as defined by Section 39.151, Utilities Code.

Sec. 2059.058. TRANSITION TO THE CENTER. (a) The department shall 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.

(b) Before the construction and operation of the center, the department may provide network security services through agreements with entities that provide those services using existing network security centers or operations.

(c) If the state agency or entity pays its proportional share of the network security services costs under this chapter, the department shall 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.

(d) This section expires September 1, 2011.

[Sections 2059.059-2059.100 reserved for expansion]

SUBCHAPTER C. NETWORK SECURITY CENTER

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

Sec. 2059.102. MANAGEMENT AND USE OF NETWORK SECURITY SYSTEM. (a) The department shall manage the operation of network security system services for all state agencies at the center.

(b) The department shall fulfill the network security requirements of each state agency to the extent practicable.

However, the department shall 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.

(c) All state agencies shall use the network security services provided through the center to the fullest extent possible.

(d) A state agency may not purchase 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. The department shall develop an efficient process for this determination.

Sec. 2059.103. CENTER LOCATION AND PHYSICAL SECURITY. (a) The department shall locate the center at a location that has an existing secure and restricted facility, cyber-security infrastructure, available trained workforce, and supportive educational capabilities.

(b) The department shall control and monitor all entrances and critical areas to prevent unauthorized entry. The department shall limit access to authorized individuals.

(c) Local law enforcement or security agencies shall monitor security alarms at the center according to service availability.

(d) The department shall restrict operational information to personnel at the center, except as provided by Chapter 321.

Sec. 2059.104. CENTER SERVICES AND SUPPORT. (a) The department shall provide the following managed security services through the center:

(1) real-time network security monitoring to detect and respond to network security events that may jeopardize this state and the residents of this state, including vulnerability assessment services consisting of a comprehensive security posture assessment, external and internal threat analysis, and penetration testing;

(2) continuous, 24-hour alerts and guidance for defeating network security threats, including firewall preconfiguration, installation, management and monitoring, intelligence gathering, protocol analysis, and user authentication;

(3) immediate incident response to counter network security activity that exposes this state and the residents of this state to risk, including complete intrusion detection systems installation, management, and monitoring and a network operations call center;

(4) development, coordination, and execution of statewide cyber-security operations to isolate, contain, and mitigate the impact of network security incidents at state agencies;

(5) operation of a central authority for all statewide information assurance programs; and

(6) the provision of educational services regarding network security.

(b) The department may provide:

(1) 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

(2) 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. (a) The department shall 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.

(b) The department shall revise the standard operating procedures as necessary to confirm network security.

(c) Each state agency shall comply with the network security policies, guidelines, and standard operating procedures.

Sec. 2059.106. PRIVATE VENDOR. (a) The department may 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.

(b) A private vendor contracted with under this section must:

(1) have the professional experience and the proven ability to establish and maintain a security operations center, including the necessary standard operating procedures and the aptitude to specifically provide the services and capabilities described by this chapter;

(2) have the verified capability to lead and partner with other vendors through joint ventures or other arrangements;

(3) be familiar with the proprietary technologies for risk management, vulnerability management, security, and intrusion detection;

(4) have significant experience with large governmental entities;

(5) be incorporated in this state or have its principal place of business in this state; and

(6) have existing relationships with an institution of higher education and other information technology security academies that provide network security education.

[Sections 2059.107-2059.150 reserved for expansion]

SUBCHAPTER D. FINANCIAL PROVISIONS

Sec. 2059.151. PAYMENT FOR SERVICES. The department shall 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. (a) The comptroller shall establish in the state treasury a revolving fund account for the administration of this chapter. The account must be used as a depository for money received from state agencies and other entities served under this chapter. Receipts attributable to the centralized network security system must be deposited into the account and separately identified within the account.

(b) The legislature may 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.

(c) The department shall maintain in the revolving fund account sufficient amounts to pay the liabilities of the center and related network security services.

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

SECTION 2. (a) In this section, "department" means the Department of Information Resources.

(b) The department shall study the interoperability of the network security features for user-specific access as provided by this Act. As part of the study, the department shall determine the potential for interoperability of user access technology and identify resulting cost savings and security benefits to Texas. The department shall 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) The department shall 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) Not later than December 31, 2006, the department shall

file the report with:

(1) the lieutenant governor;

(2) the speaker of the house of representatives; and

(3) the chairs of the house and senate committees with primary oversight over the department.

SECTION 3. This Act takes effect September 1, 2005.

* * * * *