

By: Corte

H.B. No. 3112

Substitute the following for H.B. No. 3112:

By: Corte

C.S.H.B. No. 3112

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

1 network security services to:

2 (1) state agencies; and

3 (2) other entities by agreement as provided by Section
4 2059.057.

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

7 Sec. 2059.053. OWNERSHIP OR LEASE OF NECESSARY EQUIPMENT.

8 The department may purchase in accordance with Chapters 2155, 2156,
9 2157, and 2158 any facilities or equipment necessary to provide
10 network security services to state agencies.

11 Sec. 2059.054. RESTRICTED INFORMATION. Specific network
12 security information about a state agency may be released only to
13 officials responsible for the network, law enforcement, the state
14 auditor's office, and agency or elected officials designated by the
15 department.

16 Sec. 2059.055. RESPONSIBILITY FOR EXTERNAL AND INTERNAL
17 SECURITY THREATS. If the department provides network security
18 services for a state agency or other entity under this chapter, the
19 department is responsible for network security from external
20 threats for that agency or entity. Network security management for
21 that state agency or entity regarding internal threats remains the
22 responsibility of that state agency or entity.

23 Sec. 2059.056. BIENNIAL REPORT. (a) The department shall
24 biennially prepare a report on:

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

27 (2) the status, including the financial performance,

1 of the consolidated network security system provided through the
2 center.

3 (b) The department shall submit the report to:

4 (1) the governor;

5 (2) the lieutenant governor;

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

7 (4) the state auditor's office.

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

11 (1) a school district;

12 (2) a hospital district;

13 (3) a water district; or

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

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

19 (1) each house of the legislature;

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

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

24 (4) an independent organization, as defined by Section
25 39.151, Utilities Code.

26 Sec. 2059.058. TRANSITION TO THE CENTER. (a) The
27 department shall provide network security services for a state

1 agency if the department makes that state agency's network a part of
2 the consolidated state network through the center.

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

7 (c) If the state agency or entity pays its proportional
8 share of the network security services costs under this chapter,
9 the department shall provide network security services to that
10 state agency or other entity before the department makes the state
11 agency's network a part of the consolidated state network.

12 (d) This section expires September 1, 2011.

13 [Sections 2059.059-2059.100 reserved for expansion]

14 SUBCHAPTER C. NETWORK SECURITY CENTER

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

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

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

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

26 (d) A state agency may not purchase network security
27 services unless the department determines that the agency's

1 requirement for network security services cannot be met at a
2 comparable cost through the center. The department shall develop
3 an efficient process for this determination.

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

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

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

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

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

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

26 (2) continuous, 24-hour alerts and guidance for
27 defeating network security threats, including firewall

1 preconfiguration, installation, management and monitoring,
2 intelligence gathering, protocol analysis, and user
3 authentication;

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

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

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

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

17 (b) The department may provide:

18 (1) implementation of best-of-breed information
19 security architecture engineering services, including public key
20 infrastructure development, design, engineering, custom software
21 development, and secure web design; or

22 (2) certification and accreditation to ensure
23 compliance with the applicable regulatory requirements for
24 cyber-security and information technology risk management,
25 including the use of proprietary tools to automate the assessment
26 and enforcement of compliance.

27 Sec. 2059.105. NETWORK SECURITY GUIDELINES AND STANDARD

1 OPERATING PROCEDURES. (a) The department shall adopt and provide
2 to all state agencies appropriate network security guidelines and
3 standard operating procedures to ensure efficient operation of the
4 center with a maximum return on investment for the state.

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

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

9 Sec. 2059.106. PRIVATE VENDOR. (a) The department may
10 contract with a private vendor to build and operate the center and
11 act as an authorized agent to acquire, install, integrate,
12 maintain, configure, and monitor the network security services and
13 security infrastructure elements.

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

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

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

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

26 (4) have significant experience with large
27 governmental entities;

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

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

6 [Sections 2059.107-2059.150 reserved for expansion]

7 SUBCHAPTER D. FINANCIAL PROVISIONS

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

13 Sec. 2059.152. REVOLVING FUND ACCOUNT. (a) The
14 comptroller shall establish in the state treasury a revolving fund
15 account for the administration of this chapter. The account must be
16 used as a depository for money received from state agencies and
17 other entities served under this chapter. Receipts attributable to
18 the centralized network security system must be deposited into the
19 account and separately identified within the account.

20 (b) The legislature may appropriate money for operating the
21 system directly to the department, in which case the revolving fund
22 account must be used to receive money due from local governmental
23 entities and other agencies to the extent that their money is not
24 subject to legislative appropriation.

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

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

4 SECTION 2. This Act takes effect September 1, 2005.