SUBJECT: Establishing a consolidated security network for state government

COMMITTEE: Defense Affairs and State-Federal Relations — committee substitute recommended

VOTE: 8 ayes — Corte, Campbell, Berman, Herrero, Hodge, Leibowitz, Merritt, Noriega

0 nays

1 absent — P. Moreno

WITNESSES: For — Nicolas Hollis, SecureInfo Corporation.

Against — None

On — Steve McGraw, Office of the Governor; Bill Perez, Department of Information Resources.

BACKGROUND: Currently, each state agency independently protects the security of its computer network system.

In 1989, the Department of Information Resources (DIR) was established to address the major aspects of information technology management. DIR is responsible for ensuring that state agencies and universities are informed of technology trends, including methods for securing information assets, that state agencies work together to create interoperable systems, that the state's electronic government portal (TexasOnline) performs flawlessly, that statewide telecommunication operations are reliable and efficient, and that the Legislature stays informed on technology issues.

DIGEST: CSHB 3112 would require DIR to provide network security services to state agencies and other government or legislative entities by agreement.

The bill would authorize DIR to establish and manage the operation of a network security center (NSC) to provide network security services to state agencies. Through the NSC, DIR would be required to provide all network security services to each state agency made a part of the

consolidated state network. DIR would be responsible for managing network security against external threats to an agency or entity for which DIR provided network security services. These agencies or entities, still would have to provide security management for internal threats.

NSC would have to provide certain services and support, including real-time network security monitoring to detect and respond to network security events that could jeopardize the state, continuous 24-hour alerts and guidance for defeating network security threats, and immediate incident response to counter threatening network security activity. NSC also would have to take action to mitigate the impact of network security incidents at state agencies and provide educational services regarding network security. It would adopt mandatory network security guidelines and standard operating procedures and provide them to all state agencies

CSHB 3112 would require DIR to establish NSC at a location with an existing secure and restricted facility, cyber-security infrastructure, available trained workforce, and supportive educational capabilities. DIR would be responsible for controlling and monitoring the premises against unauthorized entry, excluding the monitoring of security alarms, which would be handled by local law enforcement or security agencies. DIR could contract with a qualified private vendor to build and operate the center.

DIR would have to submit a biennial report to state leadership that included information on its ability to meet service objectives and other performance measures, and the status of the network security system, including the status of the financial performance.

DIR's authority to release specific network security information about a state agency would be limited to officials responsible for the network, law enforcement, the State Auditor's Office, and agency or elected officials designated by the department.

DIR could adopt rules to implement the network security services and purchase any facilities or equipment necessary to provide security services to state agencies, as allowed by the Code.

The bill would authorize DIR to bill and charge each state agency or other entity using the services of the system based on proportionate usage. The fees would be deposited in a revolving account established in the state

treasury by the comptroller and could be appropriated directly to DIR to operate the system. Additionally, DIR could apply for and use grant money offered by a federal agency or other source.

The bill would take effect on September 1, 2005.

SUPPORTERS SAY:

CSHB 3112 would change the way the state handles cyber security today by providing for a centralized security system that would enable the state to better and more efficiently protect computer networks while saving millions of dollars annually. The consolidated network security system would improve upon the current system and provide a nationwide model that would show that Texas was once again leading the way and remaining proactive in information technology protection.

The importance of information security in today's threat environment cannot be overstated. Information technology that supports core business processes is a vital asset to the state. The state has a significant amount of stored data that could be used for criminal purposes as small as identity theft and as large as a terrorist attack. The data also could be used to prevent the state from responding to a terrorist attack or a natural disaster.

Because each agency now handles the security of its computer network, data security is inconsistent and ineffective because some agencies are better able to protect against security threats. Lack of resources often results in an agency's inability properly to secure its computer network State agencies with weaker security systems create a weakest link effect, allowing for intruders to use the vulnerabilities of one agency to exploit the networks of others. A shared security system provided by CSHB 3112 would allow for development of deeper Internet technology (IT) security skills and provide better services with less risk of invasion or hacking.

Additionally, because of the frequency and cost of downtime for state networks, the state loses money each time there is an IT shutdown. Cyber defense specialists operating 24/7 would provide top of the line detection and incident response for the entire state at a lower overall cost compared to duplicating this capability for individual agencies.

OPPONENTS SAY:

CSHB 3112 would authorize DIR to release specific network security information about a state agency, limited to, among others, officials responsible for the network and agency or elected officials designated by DIR. Because the security data are vital, highly sensitive information, the

bill should more clearly define the officials who would be responsible for the network, which agency or elected officials would have access to the information, as well as what information would be allowed to be released.

NOTES:

The committee substitute modified the original bill by allowing the State Auditor's Office to receive specific network security information about a state agency. It also added a provision identifying what state leadership would receive the DIR's required biennial report. The substitute would provide for added managed security services by DIR through the security center and would also remove a provision giving state agency network security managers certain support through the security center.

The fiscal note reports that the bill would cost $5,200,000 through fiscal 2006-07, which would include personnel, infrastructure, and equipment costs totaling $2,300,000 in fiscal 2006 and $2,900,000 in fiscal 2007.