SUBJECT: Modifying computer network security procedures for state agencies

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

VOTE: 7 ayes — Corte, Noriega, Garcia, Herrero, Hodge, Merritt, Raymond

0 nays

2 absent — Escobar, Moreno

WITNESSES: For — None

Against — None

On — Bill Perez, Department of Information Resources

BACKGROUND: Government Code, sec. 552.139 exempts from public access any information related to computer network design, operation, and defense. Also exempt are assessments of vulnerability of a computer network, associated hardware, and software run by a governing body or contractor to unauthorized access or harm.

Government Code, sec. 2054.077 authorizes the information resources manager of a state agency to prepare or have prepared a report assessing the vulnerability of a computer, associated networks, software, and hardware to unauthorized access or harm. The report can be provided, on request, to the Department of Information Resources (DIR), the State Auditor's Office (SAO), and any other technology security entity approved by the Legislature to view the report. A version of this report must be prepared without any security compromising information to be furnished to the public upon request.

Government Code, sec. 2059.055 allows DIR to authorize release of confidential network security information only to those in charge of the network, law enforcement, the SAO, and other government officials. Information is confidential if it:

- contains passwords, personal identification numbers, access codes, encryptions, or other components of a state agency security system;
- is compiled or maintained by or for a government entity to prevent, detect, or investigate criminal activity; or
- is related to an assessment by or for a government entity aimed at determining network vulnerability to criminal activity.

DIGEST:

CSHB 2233 would require DIR to set vulnerability standards for computers, associated networks, software, and hardware run by state agencies and their contractors. It would require the agency annually to assess and compile a report on vulnerability of state technology resources. The agency could seek criminal background checks and would be exempt from certain public information and open meeting requirements. It also would add requirements and procedures for state agencies to report threats to the security of a computer system.

Vulnerability standards. DIR would be required to create rules to establish standards for:

- protecting computers, associated networks, software, and hardware run by state agencies and contractors from internal or external unauthorized access or harm, including alteration, deletion, damage, theft, or inappropriate use of electronically stored data;
- state agencies to perform risk assessments and compile reports that would examine any resources that transmit sensitive or critical information; and
- state agencies to implement physical security and disaster recovery requirements for systems containing sensitive or critical data, although the DIR executive director would have authority to waive or amend these standards for certain classes of servers or mainframes.

Vulnerability assessments. DIR would be required to assess, on an annual basis, agency risks, resource availability, and need for updated agency information in order to prioritize which state agencies would receive a vulnerability assessment, which would consist of DIR technicians attempting to hack through the agency's security system.

The agency annually would assess information technology security resources and practices of state agencies, including the vulnerability analysis it was required to conduct under sec. 2054.077. This information

would be submitted each year by December 31 in a confidential report to the governor, the lieutenant governor, the speaker of the house, and SAO. The SAO would use any vulnerability assessments and supporting information in conducting agency risk assessments, but this information would be exempt from disclosure laws.

The bill would amend Government Code, sec. 2054.077 to require an agency's information resources manager to prepare or have prepared an executive summary of the vulnerability report it currently prepares and make an electronic version of the report available upon completion – not on request as specified under current law – to the DIR, SAO, the agency's executive director, and any other technology security entity approved by the Legislature to view the report.

Computer incidents. CSHB 2233 would add requirements for state agencies to report computer incidents, defined as any violation or imminent threat of violation of state government computer security policies, acceptable use policies, or standard computer security practices. If an agency suspected criminal activity, it would be required to immediately contact DIR and appropriate law enforcement authorities. A state agency would be required to promptly investigate, document, and report to DIR any suspected or confirmed incident that:

- involved sensitive, confidential, or personally identifiable information;
- was critical in nature; or
- could be spread to other state systems.

Background checks. The bill would amend Government Code, ch. 411 to add provisions allowing DIR to seek from the Department of Public Safety or other law enforcement agencies a criminal history background that would be used only to evaluate a person who:

- was applying for a DIR job;
- would perform services for DIR; or
- worked for a contractor or subcontractor of DIR, or was applying for a job with one of those entities.

Information obtained under this section could not be released without either a court order or authorization by the subject of the background

check. Once used for the background check, all information gathered through this process would have to be destroyed by DIR.

Public information. The bill would amend Government Code, ch. 551 to remove DIR from open meetings requirements for meetings covering:

- security assessments or deployment of information resources technology;
- network security information; or
- deployment, or specifics on implementation of, security personnel, critical infrastructure, or security devices.

The bill also would amend Government Code, sec. 552.139 to expand information exempt from public access to include restricted network information under sec. 2059.055 and updated requirements of assessment reports. It also would provide for disclosure of specified information to a bidder if a governing body deemed it necessary for an accurate bid. The release of this information would not constitute voluntary disclosure under state law.

Effective date. The bill would take effect September 1, 2007. DIR would be required to establish rules governing vulnerability standards by January 1, 2008.

SUPPORTERS SAY:

CSHB 2233 would give DIR and statewide agencies additional tools and standards to ensure that vital state information and personal information was secure. The bill would complement and enhance security measures instituted during the 2005 regular session and would mandate security testing for selected agencies that either lack sufficient protection or manage highly sensitive data. Securing information and data is a constant process that evolves with changing technology, and CSHB 2233 is an attempt to ensure that a central component of state government's infrastructure remains functional and secure. By creating broad and general guidelines DIR would have to meet through rule-making, the bill would recognize the futility of trying to codify specific capabilities that could soon be obsolete.

More than 19 million incidents involving security threats were reported to DIR in fiscal 2006. The estimated cost to the state was $1.9 million and more than 8,400 in hours spent fixing problems. Although detection and antivirus protections minimized most risks and actual infections were

limited to a little more than 22,000 computers and servers, it only takes one hole in the state's security system through which a hacker could exploit and potentially expose highly sensitive information. The Legislature's approval in 2005 of HB 3112 by Corte, which created a state network operations center to prevent network hackers, was a good foundation, and CSHB 2233 would fill in holes to keep state law in line with the most current systems threats. The agency is expected to add between 10 and 15 full-time employees in the upcoming biennium to handle the increased responsibilities assigned under this bill.

Vulnerability standards. DIR would create standards that every agency would have to meet, yet through rule-making it would be able to afford greater protections to systems containing more sensitive information in lieu of a one-size-fits-all standard. Each network around the state is different, based on the type of information it contains and its size, among other things, and allowing for a flexible standard based on those factors would ensure that agencies would not have to spend needless time and/or resources increasing security if they did not house sensitive information.

Although not every contract can be reopened, some – including the one with IBM to establish a central data center – contain provisions requiring the contractor to meet current security standards, even if they have changed since the contract was signed. It also makes good business sense for any systems contractor to ensure the security of its operation.

Vulnerability assessments. Some agencies already undergo assessments by DIR, but CSHB 2233 would mandate the practice for those annually identified as the highest risk priorities. The agency estimates it would conduct roughly 90 assessments annually, in which it would attempt to hack into a system to check for holes. It would base its prioritization on a number of factors, including the type and sensitivity of data stored in a system as well as the general status of security it employed. Some larger agencies that keep large amounts of sensitive data would likely be subjected to an annual assessment, as they should, because it is vital that the state consistently and constantly ensure that its residents' important information is safe.

Although the bill would not mandate that any agency fix security flaws found through these assessments, most agencies realize they would not be well served by making vital information susceptible to theft or fraud. CSHB 2233 also would add a reporting requirement to keep an agency's

executive director apprised of security issues, which would add another layer of accountability to the process. Each agency with an information technology department already receives funding and employees to handle security, and no additional money should be necessary for these agencies to perform their tasks to meet state standards. Additionally, the majority of security problems do not require extensive time, money, or resources to fix.

Computer incidents. It is vital that DIR ensure that any threat to any network in the state system be fully investigated because one problem could quickly spread across the state. This provision is the result of a compromise with state agencies that would not impose onerous reporting requirements for every incident and would instead require that an incident met certain standards to be reported.

Background checks. Due to the sensitivity of the information DIR employees and contractors oversee, the state must be assured that these employees, including those with access to machines, are thoroughly vetted to prevent any security breach.

Public information. CSHB 2233 would exempt certain critical security information from public consumption but would provide, where applicable, for public release of certain redacted information to maintain a proper balance between the government's security interests and the public's right to know.

OPPONENTS SAY:

No one disputes the necessity of ensuring the state's information resources are well protected, but this bill would not provide the proper tools the state would need to do so. It would ask DIR to set standards, assess agency security procedures, and file a report, but would do nothing to ensure agency compliance with security standards. Creating flexible vulnerability standards could be very difficult, especially for larger agencies also governed by federal procedures and for smaller agencies without any real sensitive data.

Vulnerability standards. If the state entered into a contract with a private company and the contract did not provide for flexible security standards, the company would not be required to meet the new standards without some form of compensation, which would not be provided for under the bill.

Each network is different, and devising a flexible standards system that covered every agency yet still was effective would be very challenging. Certain agencies are governed by federal standards, which could conflict with these new standards. Other smaller agencies, or those who have seen most of their sensitive information outsourced to IBM, would not have any real need for high security standards because they would have little more than a few personal computers to protect.

Vulnerability assessments. This bill would allow DIR to identify security flaws, yet it would not compel an agency to fix them. Some might not have the time or resources to fulfill security requirements, and this bill would not provide for any additional funding or manpower with which to close any security holes.

Many agencies would be assessed annually based on the sensitivity of their information, allowing some smaller agencies to fall through the cracks. Most agencies have a Web site, allowing an avenue for outside access, and the state should attempt to assess each agency at least once in a given time period.

NOTES:

The original version of HB 2233 would have required those eligible to receive a copy of the vulnerability assessment to request it. The committee substitute specified those parties who would receive the report upon completion and added criteria for what types of incidents would have to be reported and investigated by each state agency. The substitute also delayed the implementation of DIR vulnerability standards from October 1, 2007, to January 1, 2008.

The companion bill, SB 1036 by Ellis, was reported favorably, as substituted, by the Senate Government Organization Committee on April 10 and was placed on Thursday's Local and Uncontested Calendar.