SUBJECT: DIR criminal history checks and public information security exceptions

COMMITTEE: Defense and Veterans' Affairs — committee substitute recommended

VOTE: 6 ayes — Corte, Vaught, Edwards, Farias, Pickett, C. Turner

0 nays

3 absent — Chavez, Maldonado, Ortiz

WITNESSES: For — None

Against — None

On — William Perez, Department of Information Resources

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

Government Code, sec. 2059.055 states that confidential network security information may be released by the Department of Information Resources (DIR) to officials responsible for the network, law enforcement, the State Auditor's Office (SAO), and agency or elected officials designated by the department. Information is confidential if it is:

- related to passwords, personal identification numbers, access codes, encryption, or other components of the security system of a state agency;
- collected, assembled, or maintained by or for a governmental entity to prevent, detect, or investigate criminal activity; or,
- related to an assessment, made by or for a governmental entity or maintained by a governmental entity, of the vulnerability of a network to criminal activity.

Government Code, sec 2054.077 authorizes the information resources manager of a state agency to prepare or have prepared a vulnerability

report that assesses the extent to which a computer or related program, network, system, software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm. The report can be provided, on request, to the DIR, SAO, and any other information technology security entity authorized by the Legislature to receive the report. A summary version of this report must be prepared without any security-compromising information and made available to the public on request.

DIGEST:

CSHB 1830 would allow DIR to receive criminal history information for its employees, contractors, and applicants and would exempt it 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.

Background checks. CSHB 1830 would amend Government Code, ch. 411 to allow DIR to receive criminal history from the Department of Public Safety (DPS) or the Federal Bureau of Investigation (FBI) for a person who:

- was an employee, applicant for employment, contractor, subcontractor, intern, or other volunteer with DIR or with a contractor or subcontractor for DIR; and,
- provided network security services.

DIR would be added to the list of state entities that could receive criminal history from a criminal justice agency that was the subject of an order of nondisclosure.

Criminal history obtained by DIR would not be released or disclosed except by a court order or with the consent of the person who was the subject of the information. DIR would have to destroy criminal history after the information was used to make an employment decision or to take a personnel action relating to the person who was the subject of the information.

DIR also could not obtain criminal history unless it first adopted policies and procedures stating that evidence of a criminal conviction or other relevant information from the criminal history would not automatically disqualify an individual from employment. These policies and procedures would have to outline that the hiring official would determine on a case-

by-case basis whether the individual was qualified for employment based on factors that included:

- the specific duties of the position;
- the number of offenses committed by the individual;
- the nature and seriousness of each offense;
- the length of time between the offense and the employment decision;
- the efforts by the individual at rehabilitation; and,
- the accuracy of the information on the individual's employment application.

Public information. CSHB 1830 would amend Government Code, ch. 551, and exempt DIR's governing board from open meeting requirements covering:

- security assessments or deployments relating to information resources technology;
- network security information; or,
- the deployment, or specific occasions for implementation, of security personnel, critical infrastructure, or security devices.

The bill also would amend Government Code, sec. 552.139 to exempt from public access restricted network information under sec. 2059.055 and update 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.

Vulnerability assessments. 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 to make an electronic version of the report available when it was completed – 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.

The bill would take effect September 1, 2009.

SUPPORTERS SAY:

CSHB 1830 would enhance DIR's security program and provide assurance on the background of its employees and contractors as well as those providing network security for state agencies. The bill would complement and enhance security measures instituted during the 2005 regular session with enactment of HB 3112 by Corte, which created a state network operations center to prevent network hackers.

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

Public information. CSHB 1830 would exempt certain critical security information from public consumption but would provide, when 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.

Vulnerability assessments. CSHB 1830 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.

OPPONENTS SAY:

Privacy concerns regarding the criminal history of DIR employees or contractors could arise if the agency did not properly follow the law. It also could be difficult to identify successfully those individuals providing network security services to state agencies, which could allow information on unrelated individuals to be collected accidentally and unnecessarily.

NOTES:

The original version of HB 1830 would have allowed DIR to obtain criminal history from DPS or another appropriate law enforcement agency, instead of the DPS or the FBI as in the committee substitute. The committee substitute specifies the individuals on which DIR would be allowed to collect criminal history information. It also would narrow the scope of use of criminal history information to employment decisions and personnel actions by DIR, require DIR to adopt policies and procedures before obtaining criminal history information, and introduce factors for qualified employment for individuals with criminal histories.

The companion bill, SB 2164 by Ellis, has been referred to the Senate Government Organization Committee. A similar bill, HB 2233 by Corte, passed the House during the 2007 regular session and was reported

favorably as substituted by the Senate Government Organization Committee and recommended for the Local and Uncontested Calendar, but died when the Senate did not consider it.