

BILL ANALYSIS

C.S.S.B. 532
By: Nelson
Appropriations
Committee Report (Substituted)

BACKGROUND AND PURPOSE

Interested parties suggest that state information technology decision makers need to be made aware of the latest improvements in cybersecurity and related cost efficiencies and that both the collection and reporting of state data security information warrant improvement. C.S.S.B. 532 seeks to address these issues by, among other provisions, providing for an information technology infrastructure report.

CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

RULEMAKING AUTHORITY

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

ANALYSIS

C.S.S.B. 532 amends the Government Code to require the Department of Information Resources (DIR) to collect from each state agency, other than public institutions of higher education and public university systems, certain specified information on the status and condition of the agency's information technology infrastructure and to require each applicable state agency to provide such information to DIR according to a schedule determined by DIR. The bill requires DIR to submit, not later than November 15 of each even-numbered year, a consolidated report of such information to the governor, the chair of the house appropriations committee, the chair of the senate finance committee, the speaker of the house of representatives, the lieutenant governor, and the staff of the Legislative Budget Board. The bill requires the report to include an analysis and assessment of each state agency's security and operational risks and, for a state agency found to be at higher security and operational risks, to include a detailed analysis of, and an estimate of the costs to implement, the requirements for the agency to address the risks and related vulnerabilities and the agency's efforts to address the risks through the modernization of information technology systems, use of cloud services, and use of a statewide technology center established by DIR. The bill makes the report public information and requires the report to be released or made available to the public on request, with the exception of information that is confidential under state or federal law. The bill authorizes a governmental body to withhold such confidential information without the necessity of requesting a decision from the attorney general under state public information law.

C.S.S.B. 532 makes information directly arising from a governmental body's routine efforts to prevent, detect, or investigate a computer security incident, including information contained in or derived from an information security log, confidential under state public information law, and expressly disqualifies for such confidential information related to a breach of system security as

defined in the Identity Theft Enforcement and Protection Act.

C.S.S.B. 532 changes the deadline by which a state agency is required to complete a review of the operational aspects of the agency's information resources deployment following instructions developed by DIR from not later than December 1 of each odd-numbered year to not later than March 31 of each even-numbered year.

C.S.S.B. 532 removes a state agency's discretion to consider cloud computing service options when making purchases for a major information resources project under the Information Resources Management Act and instead requires a state agency to do so. The bill specifies that consideration of those service options includes consideration of any security benefits and replaces consideration of the inclusion of any cost associated with purchasing the service options with consideration of any cost savings associated with purchasing the service options from a cloud computing service provider and from a statewide technology center established by DIR. The bill requires DIR, using existing resources, to submit not later than November 15 of each even-numbered year a report on the use of cloud computing service options by state agencies to the governor, the lieutenant governor, and the speaker of the house of representatives. The bill requires the report to include use cases that provided cost savings and other benefits and requires a state agency to cooperate with DIR in the creation of the report by providing timely and accurate information and any assistance required by DIR.

EFFECTIVE DATE

September 1, 2017.

COMPARISON OF SENATE ENGROSSED AND SUBSTITUTE

While C.S.S.B. 532 may differ from the engrossed in minor or nonsubstantive ways, the following comparison is organized and formatted in a manner that indicates the substantial differences between the engrossed and committee substitute versions of the bill.

SENATE ENGROSSED

SECTION 1. Section 552.139(b), Government Code, is amended to read as follows:

(b) The following information is confidential:

- (1) a computer network vulnerability report;
- (2) any other assessment of the extent to which data processing operations, a computer, a computer program, network, system, or system interface, or software of a governmental body or of a contractor of a governmental body is vulnerable to unauthorized access or harm, including an assessment of the extent to which the governmental body's or contractor's electronically stored information containing sensitive or critical information is vulnerable to alteration, damage, erasure, or inappropriate use; ~~and~~
- (3) a photocopy or other copy of an

HOUSE COMMITTEE SUBSTITUTE

SECTION 1. Section 552.139, Government Code, is amended by amending Subsection (b) and adding Subsection (b-1) to read as follows:

(b) Except as provided by Subsection (b-1), ~~the~~ ~~[The]~~ following information is confidential:

- (1) a computer network vulnerability report;
- (2) any other assessment of the extent to which data processing operations, a computer, a computer program, network, system, or system interface, or software of a governmental body or of a contractor of a governmental body is vulnerable to unauthorized access or harm, including an assessment of the extent to which the governmental body's or contractor's electronically stored information containing sensitive or critical information is vulnerable to alteration, damage, erasure, or inappropriate use; ~~and~~
- (3) a photocopy or other copy of an

identification badge issued to an official or employee of a governmental body; and
(4) information collected, assembled, or maintained by or for a governmental entity to prevent, detect, or investigate a security incident related to computerized data.

SECTION 2. Subchapter C, Chapter 2054, Government Code, is amended by adding Section 2054.068 to read as follows:

Sec. 2054.068. INFORMATION TECHNOLOGY INFRASTRUCTURE REPORT. (a) In this section, "information technology" includes information resources and information resources technologies.

(b) The department shall collect from each state agency information on the status and condition of the agency's information technology infrastructure, including information regarding:

(1) the agency's information security program;

(2) an inventory of the agency's servers, mainframes, and other information technology equipment;

(3) identification of vendors that operate and manage the agency's information technology infrastructure; and

(4) any additional related information requested by the department.

(c) A state agency shall provide the information required by Subsection (b) to the department according to a schedule determined by the department.

(d) Not later than November 15 of each even-numbered year, the department shall submit to the governor, chair of the house appropriations committee, chair of the senate finance committee, speaker of the house of representatives, lieutenant governor, and staff of the Legislative Budget Board a consolidated report of the information submitted by state agencies under Subsection (b).

(e) The consolidated report required by Subsection (d) must:

(1) include an analysis and assessment of each state agency's security and operational risks; and

identification badge issued to an official or employee of a governmental body; and
(4) information directly arising from a governmental body's routine efforts to prevent, detect, or investigate a computer security incident, including information contained in or derived from an information security log.

(b-1) Subsection (b) does not apply to information related to a breach of system security as defined by Section 521.053, Business & Commerce Code.

SECTION 2. Subchapter C, Chapter 2054, Government Code, is amended by adding Section 2054.068 to read as follows:

Sec. 2054.068. INFORMATION TECHNOLOGY INFRASTRUCTURE REPORT. (a) In this section, "information technology" includes information resources and information resources technologies.

(b) The department shall collect from each state agency information on the status and condition of the agency's information technology infrastructure, including information regarding:

(1) the agency's information security program;

(2) an inventory of the agency's servers, mainframes, cloud services, and other information technology equipment;

(3) identification of vendors that operate and manage the agency's information technology infrastructure; and

(4) any additional related information requested by the department.

(c) A state agency shall provide the information required by Subsection (b) to the department according to a schedule determined by the department.

(d) Not later than November 15 of each even-numbered year, the department shall submit to the governor, chair of the house appropriations committee, chair of the senate finance committee, speaker of the house of representatives, lieutenant governor, and staff of the Legislative Budget Board a consolidated report of the information submitted by state agencies under Subsection (b).

(e) The consolidated report required by Subsection (d) must:

(1) include an analysis and assessment of each state agency's security and operational risks; and

(2) for a state agency found to be at higher security and operational risks, include a detailed analysis of the requirements for the agency to address the risks and related vulnerabilities and the cost estimates to implement those requirements.

(f) With the exception of information that is confidential under Chapter 552, including Section 552.139, or other state or federal law, the consolidated report submitted under Subsection (d) is public information and must be released or made available to the public on request. A state agency may withhold information confidential under Chapter 552, including Section 552.139, or other state or federal law that is contained in a consolidated report released under this subsection without requesting a decision from the attorney general under Subchapter G, Chapter 552.

(g) This section does not apply to an institution of higher education or university system, as defined by Section 61.003, Education Code.

SECTION 3. Section 2054.0965(a), Government Code, is amended to read as follows:

(a) Not later than March 31 [~~December 1~~] of each even-numbered [~~odd-numbered~~] year, a state agency shall complete a review of the operational aspects of the agency's information resources deployment following instructions developed by the department.

SECTION 4. Section 2157.007, Government Code, is amended by amending Subsection (b) and adding Subsection (e) to read as follows:

(b) A state agency shall [~~may~~] consider cloud computing service options, including any cost savings associated with purchasing those service options from a cloud computing service provider and from a statewide technology center established by the department, when making purchases for a major information resources project under

(2) for a state agency found to be at higher security and operational risks, include a detailed analysis of, and an estimate of the costs to implement, the:

(A) requirements for the agency to address the risks and related vulnerabilities; and

(B) agency's efforts to address the risks through the:

(i) modernization of information technology systems;

(ii) use of cloud services; and

(iii) use of a statewide technology center established by the department.

(f) With the exception of information that is confidential under Chapter 552, including Section 552.139, or other state or federal law, the consolidated report submitted under Subsection (d) is public information and must be released or made available to the public on request. A governmental body as defined by Section 552.003 may withhold information confidential under Chapter 552, including Section 552.139, or other state or federal law that is contained in a consolidated report released under this subsection without the necessity of requesting a decision from the attorney general under Subchapter G, Chapter 552.

(g) This section does not apply to an institution of higher education or university system, as defined by Section 61.003, Education Code.

SECTION 3. Same as engrossed version.

SECTION 4. Section 2157.007, Government Code, is amended by amending Subsection (b) and adding Subsection (e) to read as follows:

(b) A state agency shall [~~may~~] consider cloud computing service options, including any security benefits and cost savings associated with purchasing those service options from a cloud computing service provider and from a statewide technology center established by the department, when making purchases for a major information

Section 2054.118.

(e) Not later than November 15 of each even-numbered year, the department, using existing resources, shall submit a report to the governor, lieutenant governor, and speaker of the house of representatives on the use of cloud computing service options by state agencies. The report must include use cases that provided cost savings and other benefits, including security enhancements. A state agency shall cooperate with the department in the creation of the report by providing timely and accurate information and any assistance required by the department.

SECTION 5. Section 552.139(b), Government Code, as amended by this Act, applies only to a request for public information received on or after the effective date of this Act. A request received before the effective date of this Act is governed by the law in effect when the request was received, and the former law is continued in effect for that purpose.

SECTION 6. This Act takes effect September 1, 2017.

resources project under Section 2054.118.

(e). Same as engrossed version.

SECTION 5. Same as engrossed version.

SECTION 6. Same as engrossed version.