

BILL ANALYSIS

C.S.H.B. 1604
By: Blanco
Government Transparency & Operation
Committee Report (Substituted)

BACKGROUND AND PURPOSE

Interested parties contend that the requirements for each state agency's information security plan should be strengthened in the interest of accountability. C.S.H.B. 1604 seeks to increase accountability by revising those requirements.

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.H.B. 1604 amends the Government Code to require the executive head and chief information security officer of each state agency to annually review and approve in writing the agency's information security plan and strategies for addressing the agency's information resources systems that are at highest risk for security breaches. The bill requires the highest ranking information security employee for a state agency to review and approve the plan and strategies if the agency does not have a chief information security officer. The bill establishes that the executive head retains full responsibility for the agency's information security and any risks to that security. The bill requires a state agency to file with the governing board of the Department of Information Resources the written approval for each year of the current state fiscal biennium before submitting to the Legislative Budget Board a legislative appropriation request for a state fiscal biennium.

C.S.H.B. 1604 requires each state agency to include in the agency's information security plan the actions the agency is taking to incorporate into the plan the core functions of "identify, protect, detect, respond, and recover" as recommended in a specified U.S. Department of Commerce National Institute of Standards and Technology publication. The bill requires the agency, at a minimum, to identify any information the agency requires individuals to provide to the agency or the agency retains that is not necessary for the agency's operations. The bill authorizes the agency to incorporate the core functions over a period of years. The bill requires a state agency's information security plan to include appropriate privacy and security standards that, at a minimum, require a vendor who offers cloud computing services or other software, applications, online services, or information technology solutions to any state agency to demonstrate that data provided by the state to the vendor will be maintained in compliance with all applicable state and federal laws and rules.

EFFECTIVE DATE

September 1, 2017.

COMPARISON OF ORIGINAL AND SUBSTITUTE

While C.S.H.B. 1604 may differ from the original in minor or nonsubstantive ways, the following comparison is organized and formatted in a manner that indicates the substantial differences between the introduced and committee substitute versions of the bill.

INTRODUCED

SECTION 1. Section 2054.133, Government Code, is amended by adding Subsection (b-1) to read as follows:

(b-1) The state agency shall include in the agency's information security plan a written statement signed by the executive head of the agency acknowledging that the executive head is aware of the vulnerabilities and risks identified in the plan's development.

HOUSE COMMITTEE SUBSTITUTE

SECTION 1. Section 2054.133, Government Code, is amended by adding Subsections (b-1), (b-2), (b-3), and (b-4) to read as follows:

(b-1) The executive head and chief information security officer of each state agency shall annually review and approve in writing the agency's information security plan and strategies for addressing the agency's information resources systems that are at highest risk for security breaches. If a state agency does not have a chief information security officer, the highest ranking information security employee for the agency shall review and approve the plan and strategies. The executive head retains full responsibility for the agency's information security and any risks to that security.

(b-2) Before submitting to the Legislative Budget Board a legislative appropriation request for a state fiscal biennium, a state agency must file with the board the written approval required under Subsection (b-1) for each year of the current state fiscal biennium.

(b-3) Each state agency shall include in the agency's information security plan the actions the agency is taking to incorporate into the plan the core functions of "identify, protect, detect, respond, and recover" as recommended in the "Framework for Improving Critical Infrastructure Cybersecurity" of the United States Department of Commerce National Institute of Standards and Technology. The agency shall, at a minimum, identify any information the agency requires individuals to provide to the agency or the agency retains that is not necessary for the agency's operations. The agency may incorporate the core functions over a period of years.

(b-4) A state agency's information security

plan must include appropriate privacy and security standards that, at a minimum, require a vendor who offers cloud computing services or other software, applications, online services, or information technology solutions to any state agency to demonstrate that data provided by the state to the vendor will be maintained in compliance with all applicable state and federal laws and rules.

SECTION 2. Section 2054.133(b-1), Government Code, as added by this Act, applies only to an information security plan submitted on or after the effective date of this Act.

SECTION 3. This Act takes effect September 1, 2017.

SECTION 2. Section 2054.133, Government Code, as amended by this Act, applies only to an information security plan submitted on or after the effective date of this Act.

SECTION 3. Same as introduced version.