BILL ANALYSIS

C.S.H.B. 1723
By: Raymond
International Relations & Economic Development
Committee Report (Substituted)

BACKGROUND AND PURPOSE

Small businesses that are strained for resources and expertise are vulnerable to catastrophic cybercrime. C.S.H.B. 1723 seeks to address the risks posed to small businesses concerning failures to adequately protect against cybersecurity risks and threats. The bill directs the Department of Information Resources to conduct a study, in collaboration with the Texas Workforce Commission, to assess how small businesses can improve their cybersecurity practices, determine best practices used by small businesses for cybersecurity, and determine the feasibility of establishing a grant program.

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. 1723 requires the Department of Information Resources (DIR), in collaboration with the Texas Workforce Commission (TWC), to conduct a study to determine the following:

- how small businesses can improve their ability to protect against cybersecurity risks and threats to the businesses' supply chain and to mitigate and recover from cybersecurity incidents; and
- the feasibility of establishing a grant program for small businesses to receive funds to upgrade their cybersecurity infrastructure and to participate in cybersecurity awareness training.

C.S.H.B. 1723 authorizes DIR, if necessary and as appropriate, to partner with a nonprofit entity or public institution of higher education to conduct the study. The study may be limited to the geographic region or regions served by a nonprofit entity or institution of higher education with which DIR partners. DIR, in conducting the study, may consider the following:

- the current best practices used by small businesses for cybersecurity controls for their information systems to protect against supply chain vulnerabilities, which may include best practices related to:
    - software integrity and authenticity; and
    - vendor risk management and procurement controls, including notification by vendors of any cybersecurity incidents related to the vendor's products and services;
- barriers or challenges for small businesses in purchasing or acquiring cybersecurity products or services;

- the estimated cost of any available tax incentives or other state incentives to increase the ability of small businesses to acquire products and services that promote cybersecurity;
- the availability of resources small businesses need to respond to and recover from a cybersecurity event;
- the impact of cybersecurity incidents that have affected small businesses, including the resulting costs to small businesses;
- to the extent possible, any emerging cybersecurity risks and threats to small businesses resulting from the deployment of new technologies; and
- any other issues DIR and TWC determine would have a future impact on cybersecurity for small businesses with supply chain vulnerabilities.

In determining the feasibility of establishing a grant program, the study must:

- identify the most significant and widespread cybersecurity incidents impacting small businesses, vendors, and others in the supply chain network of small businesses;
- consider the amount small businesses currently spend on cybersecurity products and services and the availability and market price of those services; and
- identify the type and frequency of training necessary to protect small businesses from supply chain cybersecurity risks and threats.

C.S.H.B. 1723 requires DIR, not later than December 31, 2024, to submit to the standing committees of the senate and house of representatives with jurisdiction over small businesses and cybersecurity a report, which must be made available on the DIR website, that contains the following:

- the results of the study, including the feasibility of establishing a grant program; and
- recommendations for best practices and controls for small businesses to implement in order to update and protect their information systems against cybersecurity risks and threats.

C.S.H.B. 1723 expires September 1, 2025.

EFFECTIVE DATE

On passage, or, if the bill does not receive the necessary vote, September 1, 2023.

COMPARISON OF INTRODUCED AND SUBSTITUTE

While C.S.H.B. 1723 may differ from the introduced in minor or nonsubstantive ways, the following summarizes the substantial differences between the introduced and committee substitute versions of the bill.

The substitute, but not the introduced, provides that the study may be limited to the geographic region or regions served by a nonprofit entity or institution of higher education with which DIR may partner to conduct the study.

The substitute and introduced both set out the same matters to be contemplated by the study but the substitute authorizes DIR to consider those matters while the introduced required those matters to be, respectively, considered, identified, considered and estimated, and assessed by DIR.