Commerce Committee
JOINT FAVORABLE REPORT

Bill No.: HB-6607
Title: AN ACT INCENTIVIZING THE ADOPTION OF CYBERSECURITY STANDARDS FOR BUSINESSES.
Vote Date: 3/22/2021
Vote Action: Joint Favorable Change of Reference to Judiciary
PH Date: 3/18/2021
File No.: 714 (598)

Disclaimer: *The following JOINT FAVORABLE Report is prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and does not represent the intent of the General Assembly or either chamber thereof for any purpose.*

SPONSORS OF BILL:

Commerce Committee

REASONS FOR BILL:

HB 6607 incentivizes businesses to adopt cybersecurity programs, to increase protections for online businesses and transactions.

RESPONSE FROM ADMINISTRATION/AGENCY:

1. **Lee Ross, Administrative Advisor, Department of Administrative Services:** Provided written testimony about this bill. The Administration concurs that this bill addresses an important issue and is generally supportive of encouraging businesses to improve their cybersecurity. After reviewing the bill, they have several technical questions and suggestions. They would appreciate the opportunity to engage in conversation on this topic if this bill moves ahead in the legislative process.

NATURE AND SOURCES OF SUPPORT:

1. **Curtis W. Dukes, Executive Vice President & General Manager, Center of Internet Security, Inc:** Provided both written and public hearing testimony in support of this bill. In his testimony, Mr. Dukes provides an overview of cybersecurity in the United States. He notes that currently, there is no national statutory standard minimum of information security. He views this bill as a critical interim step because it incentivizes the voluntary adoption of cybersecurity best practices. Mr. Dukes urges the General Assembly to pass this bill.

2. **John Keane, Legislative and Regulatory Specialist, Association of Home Appliance Manufacturers:** Provided written testimony about this bill, which they will support if it is amended. While they support the bill's intent, they believe that the bill should establish safe harbors for all covered entities that shield them from unnecessary tort or civil lawsuits when a data breach occurs if they implemented a cybersecurity program. They also request that the bill be amended to cite additional examples of standards, guidelines, and security baselines that would constitute a responsible threshold for cybersecurity. In their testimony, they outline what those different guidelines are.

3. **John P. McGloughlin, Founder & CEO, GuardSight Inc.:** Provided written testimony in support of this bill. He views this bill as a reasonable public policy measure that will encourage companies to adopt cybersecurity standards. By adopting those standards, companies will help protect both their data and their customers' data. Mr. McGloughlin appreciates the fact that this bill provides incentives to companies rather than impose penalties. He believes that this is a business-friendly approach that will make Connecticut more attractive to companies and help create jobs.

4. **Justin Orcutt:** Provided written testimony about this bill. Mr. Orcutt supports this bill's intent but believes there are multiple ways to improve it. One of his recommendations pertains to adding recognized cybersecurity frameworks. His other suggestion concerns the shield provision in the bill. In his testimony, he explains what specific frameworks he recommends and how he would alter the incentive program within the bill.

5. **Ashley Zane, Government Affairs Associate, Connecticut Business and Industry Association:** Provided both written and public hearing testimony in support of this bill. They note that cybersecurity is expensive but increasingly important as businesses have moved to a remote and online world. The CBIA believes that this bill creates a clear-cut return on investment for companies that choose to adopt the bill's cybersecurity standards. Additionally, they view the frameworks within the bill as solid and well regarded within the cybersecurity community. The CBIA suggests that the legislature keep an open mind to other frameworks that meet the required safeguards or are better suited for specific industries as this space advances.

NATURE AND SOURCES OF OPPOSITION:

None Expressed

Reported by: Peter B. Andrews **Date: 4-5-21**