Testimony of Justin Orcutt
Regarding:
HB 6607: An Act Incentivizing the Adoption of Cyber Security Standards for Businesses
Commerce Committee
March 18, 2021

Chairs Hartley and Simmons, Ranking Members Martin and Buckbee, and members of the Commerce Committee, I support the bill's intent but believe there are opportunities to improve the bill by adding recognized cybersecurity frameworks that are already required to be in place by CT businesses. In addition, the same shields should be extended to companies that have had their cybersecurity program audited by an independent third party.

Within section (1)(A) I recommend adding one additional specific framework. In CT 5.7% of our state GDP comes from DoD contracts. As of 2020 those contractors have to comply with the US Department of Defense (DoD) Cybersecurity Maturity Model (CMMC) which is a certification program managed by the (DoD) for all DoD suppliers that come in contact with certain data sets.

On line 72 of bill 6607 I propose adding "(vii) The Cyber Security Model Certification at Level 3 and above as defined by the Office of the Under Secretary of Defense for Acquisition and Sustainment".

Similar laws in Utah and Ohio have not yet addressed CMMC which over 300,000 businesses will be certified against by 2026 per DoD.

By adopting an amendment to recognize CMMC, you would be sending a clear message to the 300,000 DoD suppliers that CT is a business-friendly state for DoD contractors to conduct business. CMMC is a regulatory requirement for these companies. Connecticut is currently the country's leader in advanced manufacturing. Many of these manufacturers need to comply with CMMC and the proposed amendment will demonstrate continued support for these manufacturers.

CT would be the first state to add CMMC clause to their cyber incentive programs. CMMC would be the only framework on the bill that a company would "certify" against via an independent third party. Since businesses in CT will already be complying with CMMC the additional language acknowledges their hard work and provides those companies with equal protections without additional burden. In addition, adding a clause to recognize CMMC would create additional publicity for the bill thus helping get the word out about the bill. This ultimately would help increase adoption of cybersecurity programs by companies which helps protect the consumer in CT.

Since this is a voluntary program you are giving businesses the incentive to do the right thing and protect consumer information by following nationally recognized standards. If businesses implement the recommended frameworks in this bill they have the possibility of mitigating by 83% of all attack techniques described in the MITRE ATT&CK Framework according to the Center for Internet Security.

The bill as written recognizes NIST 800-171 which can be considered an earlier version to CMMC, however, NIST 800-171 is not CMMC. CMMC practices map to NIST 800-171 but it is different.

CMMC Level 3 encompasses 100% of NIST 800-171 but adds an additional 21 controls and requires an independent third-party audit.

In addition, if the opportunity arises, I recommend further incentives or grants to help support workforce development and upskilling our current workforce.

In summary, since Bill No. 6607's intent is to incentivize the adoption of cybersecurity standards, let's align to other rules(DoD Interim Rule) going on nationally that impose requirements of business in CT. Let's recognize CMMC as a framework under this bill to support our manufacturers in the state and provide additional incentives to defense contractors to move to business to CT. Let's provide the same support to companies that demonstrate cybersecurity practices via CMMC certification.