ASSOCIATION OF HOME APPLIANCE MANUFACTURERS

1111 19th Street NW ➢ Suite 402 ➢ Washington, DC 20036
t 202.872.5955 f 202.872.9354 www.aham.org

WRITTEN STATEMENT

JOHN KEANE
LEGISLATIVE AND REGULATORY SPECIALIST

ON BEHALF OF
THE ASSOCIATION OF HOME APPLIANCE MANUFACTURERS

CONNECTICUT GENERAL ASSEMBLY
JOINT COMMITTEE ON COMMERCE

HB 6607
RELATING TO AN ACT INCENTIVIZING THE ADOPTION OF CYBERSECURITY STANDARDS FOR BUSINESSESS

SUPPORT IF AMENDED

MARCH 18, 2021

Co-Chairs Hartley & Simmons, Vice-Chairs Cohen and Rochelle, and members of the Committee, thank you for the opportunity to share the view points of the home appliance manufacturing industry regarding the potential impacts of HB 6607.

As the industry voice, AHAM is committed to ensuring security measures for internet-connected appliances. HB 6607 allows businesses that adopt certain cybersecurity standards to plead an affirmative defense to any cause of action that alleges that a failure to implement reasonable cybersecurity controls resulted in a data breach. AHAM supports the bill's intent but also believes that the bill should also establish safe harbors so that all covered entities that implement a cybersecurity program have shields from unnecessary tort or civil lawsuits when a data breach occurs.

AHAM also believes that the NIST and federal guidelines referenced in the bill draw from and will likely continue to draw from a variety of widely accepted standards and best practices. To that end, AHAM requests an amendment to the bill that also cites the following examples of standards, guidelines, and security baselines that, if met, constitute a reasonable threshold for cybersecurity.

(i) Consensus standards that addresses commonly known or reasonably foreseeable vulnerabilities where such consensus standard is effective on the date of manufacture of the product shall be deemed a reasonable security feature or features under subdivision (a). Examples include ANSI/UL/CSA 2900 or ANSI/CTA 2088;
(ii) Security ratings from Certifying Bodies (CB) with a recognized expertise in security or connected or IoT technologies. Examples include security ratings programs at UL, Intertek, CSA, or CTIA; or
(iii) Design features that are based on widely recognized guidelines such as NISTIR 8259, the CSDE C2 Consensus Guidelines, or IEST Safe By Design - UK Code of Practice for Consumer IoT Security/ETSI TS 103 645; or
(iv) Standards and guidelines promulgated by the National Institute of Standards & Technology under the Cybersecurity Improvement Act of 2020.

These cybersecurity standards and guidelines are routinely improved and updated in order to keep pace with the development of connected devices and their applications.

In summary, following our recommendation protects all covered entities from potential liability and allows for continued reliance on existing cybersecurity protocols that provide robust security. This change would help ensure that cybersecurity protections keep pace both with innovation and the state-of-the-art in cybersecurity as they evolve to address new devices and security measures.