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

STATEMENT

KEVIN MESSNER
SENIOR VICE PRESIDENT, POLICY & GOVERNMENT RELATIONS

ON BEHALF OF
THE ASSOCIATION OF HOME APPLIANCE MANUFACTURERS

OREGON SENATE
JUDICIARY COMMITTEE

SUPPORT ONLY IF AMENDED
HB 2395, SECURITY OF INTERNET CONNECTED DEVICES

APRIL 29, 2019

Chairman Prozanski, Vice-Chair Thatcher, and members of the committee, thank you for the opportunity to share the viewpoints of the home appliance manufacturing industry regarding HB 2395, a bill addressing security features for devices connected to the Internet.

AHAM represents manufacturers of major, portable and floor care home appliances, and suppliers to the industry. Our members' ship over one million major appliances for sale in Oregon in a year and many more small appliances and floor care products. These home appliances are essential to people's lifestyle, health, safety and convenience.

AHAM's membership includes over 150 companies throughout the world. AHAM members employ tens of thousands of people and produce more than 95% of the household appliances that are shipped for sale within the United States. The factory shipment value of these products is more than $38 billion annually. Through its technology, employees and productivity, the industry contributes significantly to the US job market and the nation's economic security. Home appliances also are a success story in terms of energy efficiency and environmental protection. The purchase of new appliances often represents the most effective choice a consumer can make to reduce home energy use and costs.

As the industry voice, AHAM is committed to ensuring security measures for internet-connected appliances. To be clear, AHAM members support the objectives of reasonable cybersecurity legislation that encompasses all household connected devices and focuses on preventing an attack before it happens. Oregon should avoid the pitfalls of creating a new law that could go too far or not far enough as emerging technology develops quickly, or creates loopholes and exclusions of products that fall outside the definition of "manufacturer" and would potentially provide a weak link within the home's IoT environment.

Consensus Standards

Cybersecurity is an important issue for Oregon, but also for the US, its neighboring countries and other parts of the world. It is broadly agreed that prevention is better than after-the-fact punishment. We understand the desire by some to have punitive enforcement authority after an attack occurs. We support adding a robust preventive aspect to the bill – so both not either or. This will make the bill a better, total solution to enhancing product cybersecurity. This concept of prevention is a broadly agreed upon concept. In fact, the recently renegotiated NAFTA agreement between the US, Mexico and Canada – known as the United States-Mexico-Canada Agreement (USMCA) – has a specific Article on cybersecurity that states "Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party

Example of Government Reliance on Consensus Standards - USMCA Article 19.15: Cybersecurity

Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.

shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards."

Connected devices are so varied and developing so quickly that national consensus standards provide the most adaptable and effective way of addressing cybersecurity. Consensus standards are routinely improved and updated in order to keep pace with the development of connected devices and their applications. There is much misunderstood about consensus standards. These are used for the most important health and safety issues. For example, consensus standards are relied upon by the US Consumer Product Safety Commission for product safety, by OSHA for worker safety, for fire codes, and for building codes. The CPSC states on their website:[1]

Practice Safety by Design

- Make safety a priority at the design stage.
- Identify potential hazards and assess the risks.
- Consider foreseeable consumer use (and misuse) of the product.
- Seek to eliminate, guard against, or warn users of identified risks.
- Consult CPSC's Handbook for Manufacturing Safer Consumer Products for guidance and best practices.
- Ensure that your products meet or exceed the requirements in all applicable voluntary consensus standards ("voluntary standards").

Consensus standards are largely unknown and unseen by the public, but they are used by governments around the world for critically important issues that require continuous updates by experts in an open and transparent way. Consensus standards are developed through a consensus process involving multiple stakeholders from government, industry, advocacy groups, and others. The standards process involves checks and balances that consider inputs from multiple stakeholders. This scheme has been long-favored in the U.S., and relied on by regulators at the local, state and federal level, as well as by consumers. AHAM has developed a fact sheet on consensus standards that is attached as Appendix A.

I urge the committee to incorporate into HB 2395 a provision that recognizes that national consensus standards are an acceptable path to compliance for "reasonable security." The current version of the bill simply states essentially that "reasonable security" is protecting a connected device from unauthorized access that is appropriate for the nature and function of the connected device. That is fine, but I suspect each of the committee members may have a differing view as to what that means. And that is the problem. The bill is currently drafted so that after an attack occurs, manufacturers and the Attorney General can debate in a courtroom, possibly 10 or 20 years after a product was manufactured, what is "reasonable." We are supporting adding to that a rigorous path to compliance at the time a product is designed and manufactured. After all, security is best done at the time the product is designed. Manufacturing

[1] US Consumer Product Safety Commission. (2019). Step 6: Best Practices. Retrieved April 24, 2019, from https://www.cpsc.gov/business--manufacturing/business-education/business-guidance/BestPractices.

engineers cannot design to future court case are even to existing ones or even to differing ones that exist state by state, city by city. It is a solely focused litigious solution set up for failure.

Closing the Loophole in the Definition of Manufacturer

Every product in the home should have reasonable security features. The "network" is what needs to be secure. The network includes all devices in that network. Hackers will attack the weakest link in the network. Products made for the network essentially include three categories: original equipment manufacturers (OEMs), contracted manufacturing (or sourcing), and products that are purchased "off the shelf" and a brand placed on them. The current version of the bill excludes the last category. Any product can be a weak link in the home Internet environment that could then spread to any other product in the house that a family is using. The bill as currently drafted excludes a very important type of product category, which in turn does not fully protect the "network." Our members manufacturer products that are in the connected home and having other vulnerable products in the home that could have access to the home Internet environment is not good security for the homeowner.

Federal Guidance

The Internet is not state specific and cybersecurity is best done nationally or even internationally. The Oregon law should mirror the California law, which states that the law does not apply to any connected device that is subject to security requirements under federal law, regulations, or guidance. The current version of the bill does not include "guidance."

Other Drafting Issues

There are other drafting concerns that need to be addressed to increase clarity and reduce legal uncertainty, such as adding definitions (consensus standards, standards development organization, security feature, unauthorized access), changing 'device' to 'product,' and allowing a 'feature or features.'

In summary, AHAM strongly supports efforts to protect consumers from cybersecurity threats. We want to support a strong bill that provides incentives to design products with cybersecurity in mind and ensure every product in the home is secure. We would be pleased to work with the committee to energetically support a strong bill on cybersecurity.

APPENDIX A

FACT SHEET

NATIONAL CONSENSUS STANDARDS

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

Types of Standards

- Industry standards
- Consensus standards
- National standards
- Federal standards

What is meant by consensus standards?

- Developed through cooperation of all parties who have an interest.
- Consensus requires that all views and objections be considered, and that an effort be made toward their resolution.
- Consensus implies more than the concept of a simple majority but not necessarily unanimity.

Where are Consensus Standards Used?

- Product safety (US CPSC)
- Worker Safety (OSHA)
- Fire Safety (Fire Codes)

Example of Government Reliance on Consensus Standards - USMCA Article 19.15: Cybersecurity

Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.

What is a national standard?

A national standard is adopted by a national standards body (e.g., American National Standards Institute, Standards Council of Canada, British Standards Institution) and made available to the public. Practically speaking, however, a national standard is any standard that is widely used and recognized within a country.

Essential Requirements for National Standards

- Openness
- Lack of dominance
- Balance
- Coordination and harmonization
- Notification of standards development
- Consideration of views and objections
- Consensus vote
- Appeals
- Written procedures
- Compliance with normative ANSI policies and administrative procedures

Example of National Consensus Standard for Cyber security

UL 2900 establishes testable cybersecurity criteria for network-connectable products and systems to assess software vulnerabilities and weaknesses, minimize exploitation, address known malware, review security controls, and increase security awareness.