February 18, 2019

The Honorable Jennifer Williamson
Chair
House Committee on Judiciary
Oregon State Legislature
Salem, OR 97301

The Honorable Sherrie Sprenger
Vice Chair
House Committee on Judiciary
Oregon State Legislature
Salem, OR 97301

Re: HB2395 (at request of Attorney General Ellen Rosenblum), an act relating to security measures required for devices that connect to the Internet-- OPPOSE UNLESS AMENDED

Dear Chair Williamson and Vice Chair Sprenger:

At the outset, we would like to express our complete support for the stated objectives of HB 2395, and we have language that would achieve the bill's objectives and actually strengthen its security impact. It is critical to our industries that the total cyber-network in the home is secure and that there are no weak links. Below are some of the concerns we have with the bill's current text:

- Cybersecurity is best achieved through national consensus standards to help in the design of products to minimize vulnerabilities before the attack occurs and not in courtrooms after an attack has occurred. National consensus standards are used for other important manufacturing designs related to consumer safety. HB 2395 leaves manufacturers vulnerable to the Oregon Attorney General's interpretation of what a "reasonable security feature" years after a product is designed, manufactured and sold. What was reasonable at the time of manufacture may not seem reasonable in the future depending on the interpretation of the Attorney general at that later date. We all well-recognize that security needs to continually improve to try to stay ahead of the hackers. Debating what is "reasonable" courtroom by courtroom, jury by jury, is not effective and just diverts costs and resources away from product design and development based on the most current, expert-driven national standard. **Our recommended language would ensure that a proactive approach to cybersecurity is undertaken by recognizing national consensus standards are one of the best ways to maintain and improve the security of connected products.**
- The bill should ensure there are no weak links in the system. HB 2395 does not accomplish this because it excludes a very significant type of company: companies that "import or contract with another person." This loophole creates a perverse incentive for a company to stop manufacturing or sourcing its products (sourcing requires specific design and manufacturing specifications) in Oregon. **Our recommended language would strengthen the bill by closing this loophole in the definition of manufacturer**.
- Both state and federal regulations recognize that manufacturer's requirements for products need to be based on the date of manufacturer. HB 2395 does not. Although manufacturers actively try to

maintain a connection with their customers, it is not always possible if the consumer does not wish to remain connected to the business. For example, builders install home appliances like a refrigerator in a new house, upon purchase, the owner may not register the refrigerator with the manufacturer. **Our recommended language would ensure that the requirements of the bill would be based on the date the product was manufactured.**

- California's cybersecurity law passed last year, SB 327, included a provision that states if a federal law or regulation or guidance exists, then the bill would not be applicable. As agreed upon in the California bill, the preferred long-term goal is not be a state-by-state patchwork of differing cybersecurity laws for connected devices, but a national framework because manufacturers and connected products work across state lines. There is broad consensus in industry that this should be handled at the national level and not by a patchwork state-by-state initiative. **Our recommended language would ensure that any connected product whose functionality is subject to security provisions under federal or state law, regulations, or guidance by a federal agency, would not be applicable to this bill.**

Fiscal impact
This bill would have a significant fiscal impact to the Oregon Attorney General (AG) and local jurisdictions. There would be a huge amount of demand for guidance, and likely regulations. It is not unreasonable to assume that the AG might receive thousands of inquiries a year given the scope of this bill. The AG would need to hire experts in this area and put in place the regulatory structure costing millions of dollars. Enforcement costs also could be in the millions of dollars based on the AG's interpretation of HB2395 and the dedicated level of resources the AG identifies after their review of the enacted law during each budget cycle. A precise estimate of the potential costs does not exist, although it could be comparable to what the AG spends enforcing health and safety requirements on products.

We welcome the opportunity to discuss this bill with you further. There are serious security and technical issues involved in creating a new law in this area, and we would welcome the opportunity to bring experts in to discuss how we can jointly achieve the shared goal of increased cybersecurity. Please contact Kevin Messner at 202-872-5955 or kmessner@aham.org.

Sincerely,

Association of Home Appliance Manufacturers (AHAM)
Air-Conditioning, Heating, and Refrigeration Institute (AHRI)
The Association of Electrical Equipment and Medical Imaging Manufacturers (NEMA)
Security Industry Association (SIA)