AHAM
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

JOHN KEANE
LEGISLATIVE & REGULATORY SPECIALIST

ON BEHALF OF
THE ASSOCIATION OF HOME APPLIANCE MANUFACTURERS

HAWAII STATE LEGISLATURE
COMMITTEE ON HIGHER EDUCATION & TECHNOLOGY

SUPPORT ONLY IF AMENDED
HB 739 RELATING TO INFORMATION PRIVACY

FEBRUARY 5, 2021

Chairman Takayama and Vice Chair DeCoite and members of the Committee, thank you for the opportunity to share the view points of the home appliance manufacturing industry regarding HB 739, a bill addressing security features in connected devices.

AHAM represents manufacturers of major, portable and floor care home appliances, and suppliers to the industry. 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. The home appliance industry, through its products and innovation, is essential to consumer lifestyle, health, safety and convenience. 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 does not constrain innovation or limit consumer choice. Hawaii 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. Connected devices are also so varied and developing so quickly that is crucial to define "Internet of Things." In 2020, President Trump signed the IoT Cybersecurity Improvement Act of 2020. Under federal law (Public Law 116-207), Internet of Things devices are devices that-

> (A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and
>
> (B) can function on their own and are not only able to function when acting as a component of another device, such as a processor.

We ask that this bill includes the federal definition of "IOT Device" to ensure manufacturers are aware of what connected devices are included and maintain consistency with federal law.

Cybersecurity impacts the actual functioning of the system and is vital for consumer trust. AHAM's members have achieved great progress in the areas of appliance safety and performance through industry compliance with baseline safety standards from UL, CSA, Intertek and others as they reflect the diversity of approaches to ensure safety. Because of our experience with and track record of success in achieving increased safety and performance of our products, we believe that equipping an IoT device with a means to protect should include a security framework that are recognized by national and international safety and security institutions. We are not asking the committee to remove the other security features that it has listed in its bill, but we ask that the bill language be amended to include a security framework that is both robust and flexible. AHAM has drafted model legislative text that achieves all these goals and is attached below. This model legislative text reflects a bill that we would support. I urge the legislature to incorporate into HB 739, these standards, guidelines, and cybersecurity baselines under Section 2 below.

Cybersecurity standards are routinely improved and updated in order to keep pace with the development of connected devices and their applications. Following our recommendation allows for flexibility while ensuring security. The proposed framework 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.

The committee should also study the cybersecurity landscape fully before legislating on the issue. Not only are there gaps in state laws, such as the California law that is the model for HB 739, but there are other developments that may be at play. There is also quite a bit of activity at the federal level, including the passage of the IoT Cybersecurity Improvement Act of 2020. The National Institute for Standards & Technology, the Consumer Product Safety Commission, the Federal Trade Commission, the Federal Communications Commission, the Department of Homeland Security, and the National Telecommunications and Information Administration are all taking steps to determine the role the federal government should play in dealing with cybersecurity threats.

In summary, AHAM strongly supports efforts to protect consumers from cybersecurity threats, provided they are relevant and do not stifle innovation. The committee should have a full understanding of the issue at hand before legislating, so we ask that members first study all the activity taking place with respect to cybersecurity. Finally, should the committee still feel that legislation is necessary, the bill should reflect the importance of approved cybersecurity standards and AHAM has a model bill below that provides an effective framework for this and other areas of the bill.

The basic framework for this state model bill language is based off California's cybersecurity new law.

Section 1.

For purposes of this Act, the following terms have the following meanings:

(a) "Authorization" means a method of verifying the authority of a user, process, or device to access resources in an information system.

(b) "Consensus standards" means any standard promulgated by a nationally or industry recognized standards development organization.

(c) "IoT device" means a device that, consistent with NISTIR 8259/8259A:

> (1) has at least one tranducer (sensor or actuator) interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and
>
> (2) can function on their own and are not only able to function when acting as a component of another device, such as a processor.

(d) "Manufacturer" means the person who manufactures, imports, or contracts with another person to manufacture on the person's behalf, IoT devices that are sold or offered for sale in the state.

(e) "Reasonable security feature" means a security feature that is commensurate with the risk created by the product's level of connectivity and accounting for the cost of the product, the cost to maintain the product, and the value of the product's services to the user.

(f) "Security feature" means a feature of a product designed to provide access security for that product.

(g) "Standards development organization" means any organization that plans, develops, establishes, or coordinates standards using agreed-upon procedures, which has the following attributes: (1) openness, (2) balance of interest, (3) due process, (4) an appeals process, and (5) consensus agreement. This term includes organizations recognized by ANSI or other similar open consensus processes.

(h) “Unauthorized access, destruction, use, modification, or disclosure” means access, destruction, use, modification, or disclosure that is not authorized by the owner or authorized user.

Section 2.

(a) A manufacturer of an IoT device shall equip the product with a reasonable security feature or features, appropriate to the nature and function of the product, and the information it may collect, contain, or transmit, designed to protect the product and any information contained therein from unauthorized access, destruction, use, modification, or disclosure. Compliance with subdivisions (b) and (c) of this section fulfills the requirement of this Act to equip an IoT device with a reasonable security feature or features but compliance with subdivisions (b) and (c) of this section is not the sole sufficient method of equipping a product with a reasonable security feature.

(b) Equipping an IoT device with a means to protect the product consistent with one or more of the following:

(i) A consensus standard 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) A security rating from an Certifying Body (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.

(c) When a consensus standard is used as the basis for determining that an IoT device has been equipped with a reasonable security feature or features under subdivision (b) of this section and that consensus standard is amended, a manufacturer whose products conform to the previous version of the consensus standard shall be deemed to have equipped its IoT device with a reasonable security feature or features under subdivision (b) of this section so long as the product is manufactured not more than one year after the effective date of the amended consensus standard.

Section 3.

(a) This Act shall not be construed to (1) impose any duty upon the manufacturer of an IoT device related to unaffiliated third-party software or applications that a user chooses to add to or use to interface with an IoT device or (2) impose any duty upon the manufacturer of an IoT device with respect to software patches, updates or downloads.

(b) This Act shall not be construed to impose any duty upon the manufacturer of an IoT device to prevent a user from having full control over an IoT device, including the ability to modify the software or firmware running on the product at the user's discretion.

(c) This Act shall not apply to any IoT device whose functionality is subject to security provisions under federal or state law, regulations, standard or guidance by a federal agency.

(d) This Act shall not apply to any product for which consumer registration of an IoT device is made available by the manufacturer and the consumer fails to register the IoT device with the manufacturer.

(e) This Act shall not be construed to provide a basis for a private right of action or to be used as the basis for a standard of conduct under any other private right of action under the statutory or common law of this or any other state. This Act may be used as a basis for establishing an appropriate standard of conduct as the basis for any affirmative defense otherwise available under statutory or common law. The Attorney General shall have the exclusive authority to enforce this Act. The duties and obligations imposed by this Act are cumulative with any other duties or obligations imposed under other law and shall not be construed to relieve any party from any duties or obligations imposed under other law.

(f) Any penalties imposed under this Act shall not exceed $500,000 for the total of all violations of this Act by a manufacturer and shall be mitigated taking into account good faith efforts to comply with this Act, voluntary action to remedy any noncompliance, including through software updates, the actual harm or risk to consumers, the cost of the product, the cost to maintain the product, the value of the product's service's to the user, and other relevant factors. Any injunctive action shall be prospective and apply only to future products.

(g) Any voluntary action to remedy noncompliance with this Act shall be evaluated for reasonableness taking into account the risk created by the product's level of connectivity and accounting for the cost of the product, the cost to maintain the product, and the value of the product's services to the user.

(h) This Act shall not be construed to limit the authority of a law enforcement agency to obtain an IoT device information from a manufacturer as otherwise authorized by law or pursuant to an order of a court of competent jurisdiction.

(i) A covered entity, provider of health care, business associate, health care service plan, contractor, employer, or any other person subject to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191) or the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) shall not be subject to this Act with respect to any activity regulated by those acts.

(j) This title shall only apply to IoT device manufactured after this title becomes operative.

(k) This Act shall become operative on [INSERT DATE].