



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

October 17, 2021

Via E-Mail

Katerina N. Megas  
Applied Cybersecurity Division  
National Institute of Standards and Technology

labeling-eo@nist.gov

Re: Draft Baseline Security Criteria for Consumer IoT Devices

Ms. Megas:

On behalf of the Association of Home Appliance Manufacturers (AHAM), I would like to provide our comments on the National Institute of Standards and Technology's (NIST) Draft of Baseline Security Criteria for Consumer IoT Devices. AHAM is supportive of NIST's efforts in cybersecurity and offers some thoughts on how the document may be improved.

AHAM represents more than 150 member companies that manufacture 90% of the major, portable and floor care appliances shipped for sale in the U.S. Home appliances are the heart of the home, and AHAM members provide safe, innovative, sustainable and efficient products that enhance consumers' lives. The home appliance industry is a significant segment of the economy, measured by the contributions of home appliance manufacturers, wholesalers, and retailers to the U.S. economy. In all, the industry drives nearly \$200 billion in economic output throughout the U.S. and manufactures products with a factory shipment value of more than \$50 billion.

Because of their ubiquity, home appliances are going to be central to the connected home and any activity that arises out of this white paper will undoubtedly affect the home appliance industry. Home appliances also include a broad range of product, from refrigerators to electric toothbrushes, and therefore appliance manufacturers are acutely aware that there is no "one size fits all" solution to cybersecurity. The design of a label system should take into account the intended application at the point of design, not all possible uses across all possible sectors. Any recommendations that come from NIST must take this into account. With that in mind, AHAM offers the following broad recommendations on the white paper.

**I. Product Labels Are Already Abundant And Another Could Add To Consumer Confusion.**

The draft white paper at issue is the result of Presidential Executive Order 14028 on Improving the Nation’s Cybersecurity (issued on May 12, 2021). NIST’s analysis should take into account that products and their packaging already incorporate a variety of labels, some are required and others are voluntary.

The eventual outcome of NIST’s activity might be yet another label that manufacturers need to incorporate. As it proceeds, NIST should take into account that such a label may not meaningfully communicate its intended message to the consumer given the number of labels to which consumers are already exposed. In addition to providing criteria for a cybersecurity labeling programs, NIST should also investigate whether such programs will accomplish their intended goals of communicating meaningful information to the product’s end user. To the extent that this eventuality exists, AHAM opposes a mandatory cybersecurity label.

## **II. Any Labelling Program Should Not Focus On Any One Cybersecurity Solution**

First, any labelling program should not focus on any one cybersecurity solution. AHAM believes there are a suite of options for manufacturers to employ that provide robust cybersecurity without stifling innovation or taking into account what may be vast differences in product design, lifecycle, and security needs. AHAM developed model legislative language on cybersecurity and it reflects this principle:

“(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 EN 303.645; or
- (iv) Standards and guidelines promulgated by the National Institute of Standards & Technology under the Cybersecurity Improvement Act of 2020.”

## **III. NIST’s Recommendations Should Not Lead To A Patchwork Of Cybersecurity Requirements.**

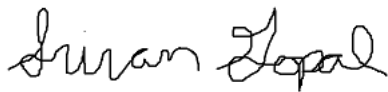
The label program should not create requirements that are not part of regional or international standards. A consensus approach is leading to broad harmonization of cybersecurity requirements and NIST’s labeling activity should not interfere with this. This may require additional resources from NIST in the form of international coordination and work in the context of regional and international standards development bodies, but such coordination is necessary for products and networks that operate globally.

#### **IV. Tiered Security Rating Systems Must Take Into Account The Nature Of The Product.**

A cyber security label scheme must address differences in product categories and the risk profiles inherent to those categories. “Bronze, Silver, Gold” labelling schemes for other programs, such as energy efficiency in buildings, but a tiered rating approach may not be suitable for all products, so it should not be required of a labeling program. Tiered cybersecurity structures may encourage consumers to view the “lower” levels of rating as inferior, but this is not a desirable outcome. A tiered system should be able to indicate the appropriate security rating for a given product. The criteria and associated label should be developed based on the use case.

AHAM appreciates the opportunity to submit these comments on NIST’s Draft Baseline Security Criteria for Consumer IoT Devices and would be glad to discuss these matters in more detail should you so request.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Sriram Gopal". The signature is fluid and cursive, with the first name being more prominent.

Sriram Gopal  
Director, Technology and Environmental Policy