



power tool institute, inc.

1300 SUMNER AVENUE, CLEVELAND, OHIO 44115-2851 216-241-7333 FAX 216-241-0105

E-Mail: [pti@powertoolinstitute.com](mailto:pti@powertoolinstitute.com) URL: [www.powertoolinstitute.com](http://www.powertoolinstitute.com)

October 15, 2021

TO: The National Institute of Standards and Technology (NIST)

Via E-Mail: [labeling-eo@nist.gov](mailto:labeling-eo@nist.gov)

SUBJECT: Power Tool Institute Comments on NIST White Paper “DRAFT Baseline Security Criteria for Consumer IoT Devices” dated August 31, 2021

The Power Tool Institute (PTI) is pleased to be provided an opportunity to submit comments to NIST on its document entitled “DRAFT Baseline Security Criteria for Consumer IoT Devices” dated August 31, 2021.

PTI is a trade association of the leading power tool manufacturers in the United States.

Our member companies include:

- Chervon North America, Inc.
- Festool USA, LLC
- Hilti, Inc.
- Koki Holdings America Ltd.
- Makita U.S.A., Inc.
- Metabo Corporation
- Robert Bosch Tool Corporation
- Stanley Black & Decker Corporation
- Stihl Incorporated
- Techtronic Industries – North America

Our comments are as follows:

**I. Comments on whether the proposed cybersecurity labeling technical criteria are appropriate for a broad range of consumer devices and whether additional criteria are needed**

Throughout the document, there are several references to “consumer IoT devices”. However it is not entirely clear what a “consumer IoT device” is. For example, there are some products that are intended for professional use only (i.e. not for consumers in general) that could be connected to a network either continuously or for very short periods of time. It is not clear if these types of products would be covered or not. Therefore, a definition of “consumer IoT devices” would add clarity to this document.

PTI believes that the simpler the labeling scheme, the better. We suggest the tiers method of indicating the amount of security be limited to something like a NIST, NIST +, NIST ++ security symbol. This is similar to the tier system used in ANSI/ISEA Z87.1, American National Standard For Occupational and Educational Personal Eye and Face Protection Devices.

## **II. Comments on whether Tables 1, 2, and 3 have the right level of detail in the discussion of the criteria to ensure consistency in meeting the cybersecurity expectations**

It is not clear what items in Tables 1-3 apply to what types of devices. For example, in the third row of Table 3 (Data Protection), it refers to “The ability to use a short-range and/or local network transmission protocol (e.g., Zigbee, Bluetooth, mDNS, LLDP, and IEEE 1905.1) to communicate with some product components as necessary”, however no mention of these short-range and/or local network transmission protocols are mentioned in Tables 1 and 2. Since many products use only this type of transmission protocol, do Tables 1 and 2 apply to them? Clarification on this point would be very useful.

PTI believes that there should be several categories of consumer IoT devices defined, with specific requirements for each category. As a starting point, we suggest the following:

Category 1 – Products with no communication activity. This would fall outside the definition of a consumer IoT device.

Category 2 – Products that only communicate with networks for the purpose of reporting status only. Subcategories could include those products permanently connected to a network and those that temporarily connect to networks.

Category 3 – Products where it is possible to adjust settings of the product through network communication, but control of the product is not possible. Subcategories could include those products permanently connected to a network and those that temporarily connect to networks.

Category 4 – Products where control of the product is possible through network communication. Subcategories could include those products permanently connected to a network and those that temporarily connect to networks.

In Table 2, first row (Documentation), it should be clarified if the proposed required documentation needs to be in a physical (e.g. paper) format or whether a digital format would be acceptable. Alternatively, would this requirement be fulfilled if the documentation was part of the Technical File for the product? In addition, who would a manufacturer be obligated to provide this documentation on request to anyone who requests it?

In Table 2, last row (Education and Awareness), the proposed requirements seem to be overly burdensome for a manufacturer of a consumer IoT device with limited network transmission capability. In these cases, it should be adequate for the manufacturer to simply describe how the device operates in the instruction manual for the product.

## **III. Comments on whether the extent to which consumer IoT devices with very limited capabilities (e.g., microcontroller-based devices) can address the criteria**

PTI believes that it would be inappropriate and overly burdensome for consumer IoT devices with very limited capabilities to have to comply with all of the proposed requirements in Tables 1-3. Please see our comments above on different categories of consumer IoT devices.

## **IV. Comments on the potential for assessment and certification of IoT product components**

PTI suggests that if the requirements for consumer IoT devices were harmonized with existing voluntary standards, then assessment and certification would be a simple matter of Nationally Recognized Testing Laboratories (NRTLs) assessing and certifying products to those standards. Please see our general comments below.

## **V. General comments**

PTI strongly suggests that it should not be required to place a label on the product itself. In many cases, a consumer IoT product may be very small in size and there is little room left for any additional labels beyond all of the markings and labels that are already required by existing safety standards. Therefore, it should be possible to place the proposed label on packaging or alternatively provide an allowance for a digital label (i.e. accessed through a QR code or other “smart” code).

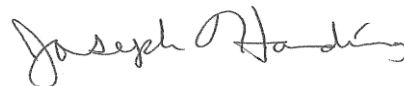
We also suggest that NIST should strongly consider harmonizing the proposed requirements for consumer IoT devices with existing published standards or regulations. A list of such standards and regulations are as follows:

- ISO/IEC TS 27100:2020, Information technology — Cybersecurity — Overview and concepts
- IEC 60335-1:2020, Household and similar electrical appliances - Safety - Part 1: General requirements (Specifically Annex R and Annex U)
- UL 2900-1, ANSI/CAN/UL Standard for Software Cybersecurity for Network-Connectable Products, Part I: General Requirements
- European ENISA Cybersecurity Act and ETSI 303 645, Cyber Security for Consumer Internet of Things: Baseline Requirements

It should be noted that many standards developing organizations are currently in the process of developing cybersecurity requirements for a wide array of products. Therefore, NIST should incorporate flexibility for the inevitable inclusion of device security into these product standards by which firmware and hardware functional restrictions may allow lower security connection, depending on the type of consumer IoT device.

In closing, PTI is grateful for the opportunity to comment on the NIST White Paper “DRAFT Baseline Security Criteria for Consumer IoT Devices”. Please feel free to contact us with any questions regarding our comments.

Sincerely,



JOSEPH HARDING  
Technical Director  
Power Tool Institute  
[jharding@thomasamc.com](mailto:jharding@thomasamc.com)

JH/sm  
pti