Consumer Technology Association™

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

August 17, 2021

To: labeling-eo@nist.gov

Consumer Technology Association (CTA) appreciates the opportunity to help NIST with its work under the Executive Order and to participate in Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software.

In this white paper, CTA addresses NIST's request for suggestions and feedback on challenges and practical approaches to initiating cybersecurity labeling efforts for Internet of Things (IoT) devices and consumer software.

We respectfully submit the attached paper as follows:

Title: Cybersecurity Labeling, Conformity Assessment and Self-Attestation (CTA)
Areas Being Addressed:

1. how different conformity assessment approaches (e.g., vendor attestation, third-party conformity assessment) can be employed in consumer software labeling efforts
2. consumer product labeling programs for educating the public on the security properties of consumer software
3. feasibility and possible means for implementing tiered labels that reflect increasingly comprehensive levels of testing and assessment

Representative: Michael Bergman
Vice president, technology & standards
Consumer Technology Association
mbergman@CTA.tech / +1(609) 865-4402

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ Michael Petricone*

Michael Petricone
Sr. VP, Government and Regulatory Affairs

/s/ Michael Bergman

Michael Bergman
Vice president, technology & standards

Consumer Technology Association
1919 S. Eads Street, Arlington, VA 22202
(703) 907-7644

CTA Position Paper On Cybersecurity Labeling, Conformity Assessment and Self-Attestation

Consumer-facing labeling for cybersecurity has been described as "similar to EnergyGuide labels", "like food nutrition labels", or other simplified approaches. Unfortunately, cybersecurity is not simple. The yellow EnergyGuide label must only convey a single quantitative and measurable value, the annual cost of power consumed.[1] Food nutrition is also quantitative and is the beneficiary of significant consumer education in schools, media and elsewhere. However, the security of software and IoT devices is not a quantifiable value like watts, dollars or percent of daily requirement. Cybersecurity is also – to the average consumer – arcane and uninteresting. The consumer expects brand reputation to be a sufficient indication of the security of the product.

Cybersecurity labeling should avoid attempts to copy other programs and build from these important requirements.

1. A cybersecurity label scheme should be based on industry consensus standards, recognizing that no single standard or set of criteria will be appropriate for all IoT device categories or use cases. The NISTIR 8259A/B[2] documents may be viewed as foundational references but are guidance documents. Developers and assessors require technical standards. There are a number of available industry documents, such as ANSI/CTA-2088[3], ETSI EN 303 645[4], and the (draft) ISO/IEC 27402[5]. Much work has been done to align these standards; ANSI/CTA-2088 is mapped to the NISTIR 8259 series via the NIST On Line Informative Reference program (OLIR).[6]

2. The label system should avoid fragmentation in the marketplace. This requires long-term international coordination and work in the context of regional and international standards development bodies such as those mentioned above. While this may seem like a challenge, it is a necessary part of making a useful label program in a global ecosystem. Industry is actively seeking such harmonization through participation in global standards discussions, regional body meetings and the like.[7] Also, some consideration should be given to mutual recognition of marks, as other regions (EU, China, Malaysia, Singapore, etc.) have similar plans or programs.

3. A cybersecurity label program should be built on risk assessment as much as security capabilities. While technical standards for cybersecurity are important parts of the solution, the program should not rely entirely on such requirements. 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. It is not feasible to consider actual applications, which can be anything the purchaser chooses.

4. The label program should not create new ad-hoc requirements that are not part of regional or international standards. Such additions would deviate from the consensus approach that led to broad acceptance of these standards in the first place. All requirements instantiated in such a program should be direct references to industry consensus standards.

---

[1] EnergyGuide actually provides the value in annual dollar cost and therms (therms per year).
[2] https://csrc.nist.gov/publications/detail/nistir/8259/final
[3] Available as a no-cost download at https://shop.cta.tech/collections/standards/cybersecurity
[4] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf
[5] https://www.iso.org/standard/80136.html
[6] https://csrc.nist.gov/Projects/olir
[7] For example, CTA presented on the merits of NISTIR 8259A and ANSI/CTA-2088 at the 2020 APEC Cybersecurity Conference in Malaysia.

5. A cyber security label scheme must be appropriate to different categories of devices and corresponding risk profiles. Security labels for "tier 1, 2, 3…" or "bronze, silver, gold…" exist in the marketplace today. What experience shows is that while such "good/better/best" programs are appropriate for other assessment categories, tiered cybersecurity structures encourage consumers to view the "lower" levels of rating as inferior. Clearly this is not a desirable outcome.

   The tiered system should be able to indicate the appropriate security rating for, e.g., a one-time-use package tracking device, a pet tracking device, a baby monitor, a consumer drone, and a consumer router. The package or pet tracking devices should not be expected to meet the requirements of a consumer router, and at the same time should not be saddled with a label that gives the impression that the device has inferior security because it is "only" a "tier 1" or "copper", etc., rating. Ratings appropriate to the risk assessment of the device should reflect that appropriateness. For example, a device class rating that embodies the tier system, with a non-tiered "this device meets standards appropriate for its tier" certification would be more appropriate than a security level rating. The criteria and associated label should be developed based on the use case.

6. Labeling should not convey a false sense of security. "Certified secure" should not convey a sense of "no new vulnerabilities, ever, and unhackable". All devices are ultimately susceptible to hacks, sooner or later. Hackers – white hat and black hat – will certainly target the labeled devices. Media reports of devices being hacked will soon begin to include label status of the device. That labeled devices can be hacked will undermine the confidence consumers have in label programs. Labels, and the corresponding consumer education campaigns, should convey exactly what they represent, that the device was designed to meet certain standards.

7. A cybersecurity label system should not assume the product package will have area for a significant amount of information. Many products are in small packages and already have limited space for existing information. A requirement for a 2"x5" (5cm x 12.5cm) label may seem innocuous but would force out other information or require smaller font than is useful for many consumers. With the ubiquity of smart phones and internet coverage, a QR code or other e-Label option that redirects to a website is a more effective option.

8. Existing conformity assessment programs should be incorporated into the pilot, not simply studied. UL[8], Eurofins Digital Testing[9], Intertek[10] and others have such programs. These programs already are based on regional industry consensus standards and are expected to adapt to international standards when available[11]. If the label pilot is to represent what is feasible and available, the program should explicitly use these programs, albeit with consideration for the points above including modification of tiered structures.

9. The label system should recognize both third party assessment and self-attestation. Third party assessment programs exist but the ecosystem cannot handle the vast number of new product introductions seen annually. Self-attestation is necessary to avoid ecosystem overload and should recognize the work of manufacturers who are currently operating via industry best practices. Large customers, including retailers, large enterprises and state and local governments should be able to accept self-attestation under this structure.

---

[8] See https://ims.ul.com/IoT-security-rating
[9] See https://www.eurofins-digitaltesting.com/cyber-security/
[10] See https://www.intertek.com/cyber-assured/
[11] Draft ISO/IEC 27402 is expected to be adopted by such programs, when it is published.

10. The label system will require end-user awareness and education. While the consumer should never be considered the primary source of security, everyone has a role to play. There should be a sense of balanced responsibility between manufacturers, retailers, installers, consumers and other customers. There must be a significant consumer education campaign if a label program is to have any real effect.

Conclusion

Developing a successful voluntary cybersecurity label pilot will be complicated. CTA urges NIST and FTC to consider the above requirements in developing a pilot label program for consumer products, whether for software or connected devices. CTA and its member companies stand ready to assist as NIST and FTC step up to this challenge.