13 October 2021

National Institute of Science and Technology
Cybersecurity for the Internet of Things (IoT) program

Ref: "**Draft IoT Device Labeling Criteria" NIST White Paper Draft**

Dear NIST IoT Labeling,

The TIC Council Americas is pleased to provide comment on the "Draft IoT Device Labeling Criteria" draft NIST white paper published on 31 August 2021. Ensuring the security of IoT capable devices is of critical importance to address the rise in cybersecurity attacks and the white paper provides beneficial information to support a robust discussion of this critical issue.

The TIC Council supports all efforts to address cybersecurity in connected infrastructure[1], systems, components and devices and looks forward to our ongoing engagement and discussion on this topic.

Using a combination of cybersecurity standards, evaluation, and certification will improve systems security and risk management. Conformity assessment is a reasonable and responsible model for addressing the challenges of acquisition and cybersecurity and improving cybersecurity posture throughout the product lifecycle. And trusted, independent third-party conformity assessment[2] is a cost-effective policy solution as it provides the highest level of confidence and helps government leverage private-sector resources.

For your review, we have included responses to each area of consideration included in the Draft IoT Device Labeling Criteria and look forward to a robust discussion with NIST and other stakeholders to identify solutions to protect our systems and infrastructure.

TIC Council is a global association representing over 90 international independent third-party testing, inspection, certification and verification organizations. Testing, Inspection and Certification (TIC) companies cater to a diverse range of industry sectors and a variety of standards and legislation. The industry represents an estimated one million employees across the world with annual sales of approximately USD 200 billion.

We appreciate the opportunity to give feedback on "Draft IoT Device Labeling Criteria" NIST white paper draft. Should you have any questions, please don't hesitate to contact Karin Athanas at +1 240 762 8069 / kathanas@tic-council.org.

Sincerely,

Hanane Taidi
Director General
TIC Council

Karin Athanas
Executive Director
TIC Council Americas
kathanas@tic-council.org

[1] https://www.tic-council.org/application/files/5915/5775/4670/IFIA_One_Pager_IoT_and_Cybersecurity.pdf
[2] https://www.tic-council.org/application/files/6016/2489/1617/2021_-_Americas_Position_on_CA_for_IoT_Final.pdf

Areas of Consideration – Draft IoT Device Labeling Criteria

1. Whether these are appropriate criteria for a broad range of consumer devices.

   If the resulting certification scheme were to allow for both vendor-attestation (1st party Suppliers Declaration of Conformity) and third-party assessment (certification), a clear distinction should be made in the labelling to differentiate the claims. When it comes to cyber security assessments, independence of the assessor has been a cornerstone to ensuring valid results, thus, the additional value of assessments/certification performed through 3rd parties should be made clear and differentiated to the consumer. If vendor-attestation (sDoC) is allowed and a tiered scheme is adopted, vendor attestation should only be acceptable at the lowest tier(s).

2. Whether additional criteria are needed, including criteria that specifically address other components of the product beyond the device.

   Applicable criteria should be defined for all components in the IoT ecosystem, the device, apps (mobile or web), and cloud services. The specific inclusion of "hub" requirements should depend on the product architecture. If the hub is a required component that provides a 1-to-1 interface between the device and the Internet, criteria for the hub should be included. However, if the hub is an optional component, or a component that can be purchased independently from the device, hub requirements should not be necessary as the hub should simply be seen as another distinct IoT device (following the criteria defined for IoT devices) with an interface to other components.

3. 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.

   No additional comments.

4. What might be the appropriate definitive text for these criteria be stated to facilitate conformity assessment.

   No additional comments.

5. The extent to which consumer IoT devices with very limited capabilities (e.g., microcontroller-based devices) can address the criteria.

No additional comments.

6. **The potential for assessment and certification of IoT product components (e.g., cloud backend, hub, mobile app) independent of one another.**

   For IoT products with common components across the ecosystem (e.g., common cloud, common app), it should be possible to reuse assessments and certification. However, there should be a minimum amount of testing of these components for each IoT product that is certified using these common backend services. Perhaps a component certification for things like cloud and apps where products that use certified components only need to include testing against a small set of product-app or product-cloud test cases whereas if the components are not individually certified, there is a broader set of cloud and app test requirements that must be met.

   Allowing component assessments also supports the existence of products that are interoperable across multiple ecosystems and avoids vendor lock-in and potentially reduces competition. Products could be certified to be approved to work with other specified components.

   "Increasingly Comprehensive Levels of Testing and Assessment (Tiers)".

   The baseline for IoT security could be scaled for the features and target environment of the consumer IoT product; determination of an appropriate tier should be based on a cost (of implementation and assessment of additional security features) weighed against the risk of the threat(s) that the tier protects against. However, at this time, I believe that tiers should be avoided within the already limited space of consumer IoT in order to "keep it simple", maximize adoption, and avoid unnecessary confusion when adopting a labeling scheme. The reasons for avoiding tiers within consumer products at this time are as follows:

   - The security capabilities and testing required to adequately secure even higher risk consumer IoT products, such as door locks or stoves, remains a relatively low bar and it should be possible, without unreasonable effort, to apply this same level of protection to all IoT, even if the risk is lower.
   - Cybersecurity standards and requirements continue to evolve. It remains unclear what security capabilities, beyond a reasonable baseline, would provide additional value for consumers (e.g. should a tier incorporate physical hardening, or MFA, or both?)
   - A consumer's understanding of cybersecurity requirements, testing, and assessment, is unlikely to be sophisticated enough to discern between tiers of testing based on levels of assurance evaluation. If a low level tier is self-assessed, this can also lead to confusion as the consumer may not understand the value of 3rd party assessment or the value of black box vs. white box testing.

- With other consumer product labeling schemes (non cyber security related) tiers have a more tangible role ("one star" "two star", etc.) to describe a feature such as energy efficiency; it is clear to the consumer that 3 star product has better efficiency than 1 star. For cyber security, it is difficult to educate the consumer about what the advanced tier provides or what additional mitigations the consumer should implement because of a low rating.