ITI Promoting Innovation Worldwide

ITI Comments on NIST White Paper on Baseline Security Criteria for Consumer IoT Device Labeling Program

October 15, 2021

The Information Technology Industry Council (ITI) appreciates the opportunity to submit the following comments on NIST's *Draft White Paper on Baseline Security Criteria for Consumer IoT Devices*. ITI is the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and represents leading companies from across the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity and Internet companies. To reap the benefits of IoT devices and to minimize the potentially significant risks posed by malicious actors seeking to exploit them, we agree with NIST and other government stakeholders around the world that these devices need to be secure and resilient.

As NIST rightly points out in the White Paper, utility for cybersecurity, feasibility of implementation, and support for labeling and conformity assessment are key factors to developing a pilot labeling program for IoT devices. ITI encourages stakeholders to take thoughtful, holistic approaches to managing both the security of devices and the networks and complex ecosystems that comprise global IoT security. In addition, ITI joined efforts with the Council to Secure the Digital Economy (CSDE) to release the IoT Security Policy Principles (2021) document[1] and noted that it would be more appropriate to consider voluntary labeling regimes for (non-sophisticated) consumer household verticals as an initial step by building upon industry frameworks and international standards. In particular, we welcome NIST's leadership in identifying key elements of existing labeling programs rather than establishing its own programs.

ITI also welcomes the release of the recent *Executive Order on Improving the Nation's Cybersecurity (EO 14028)* and appreciates the EO's intention to create digital literacy pilot programs to improve IoT and software development security. Cybersecurity is a shared responsibility, and the consumer should understand its responsibility to nonetheless protect "labeled" software and IoT devices using baseline criteria such as strong and unique passwords and applying security updates. The labeling program should be effective in improving IoT cybersecurity as consumers understand the purpose and limitations of such labeling and make market choices accordingly. We appreciate NIST's leadership and encourage NIST to continue working with industry as well as in international engagements in the policy and standards arenas.

In the White Paper, we welcome NIST's approach of examining IoT products more broadly rather than narrowly focusing on IoT devices. However, it might become tricky in some cases to define the boundaries of a specific product, and certain components may well belong to more than one IoT product. Such expansion should be considered carefully. We encourage NIST to continue focusing on IoT Device, in manner consistent with the NISTIR 8259 and 8228 series as the scope at this stage for the baseline criteria, while allowing flexibility to the IoT Device manufacturer to indicate an appropriate baseline capability is supported by a different entity in the IoT System that extends beyond the device[2].

[1] CSDE. IoT Security Policy Principles. April 2021.
[2] ISO/IEC 27402. Draft.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

ITI is committed to work with NIST to further define the scope and develop the details of the labeling program.

General Comments

Continue to Partner with Industry, Advance Global Harmonization, and Include Clear Definitions to All NISTIR Documents

The Administration's Botnet Roadmap, released at the end of 2018, and NIST's work on developing IoT baselines were positive steps to forge better collaboration between industry, government, and academia on IoT security. ITI co-founded CSDE, which published an International Anti-Botnet Guide[3] to identify practices and capabilities for combating botnets and other automated threats (a document which was cited multiple times in the Botnet Roadmap). We also participated in the CSDE-driven C2 consensus with 20 other associations to coalesce around IoT device security baselines.[4] Recently ITI joined the CSDE effort on IoT Security Policy Principles, which references and incorporates several ITI positions in this domain.

We emphasize the rapid pace of developments in IoT technology occurring in the commercial space globally, and the need for consistent and ongoing dialogues between the government and the private sector to secure IoT devices and the broader ecosystem to which they attach and impact. We recommend NIST continue advancing its efforts on IoT security domestically and globally. To achieve global harmonization, the development of international standards governing IoT security and privacy, such as device baseline requirements (ISO/IEC 27402) (in draft), presents a crucial opportunity to inform future requirements on the global stage. To ensure alignment, we encourage NIST to continue moving the international standards debate forward with key partners and allies. We also recommend NIST explicitly refer to ISO/IEC 27402 (in draft) in the document.

It is important to emphasize that any deviations from international standards can have a serious effect on global trade, such as requiring suppliers to meet different technical specifications, forcing duplication of testing and requirements, delaying the entry of goods into market, and inevitably reducing innovation and competition. With this consideration in mind, ensuring consistency with globally aligned definitions in determining the scope of IoT is essential. Below, we recommend NIST include clear definitions of IoT Product and Device in all its publications:

- **We welcome NIST's approach to focus on IoT products more broadly rather than narrowly on IoT devices for labeling considerations.** Given the fact that a consumer labeling program often grants access to additional security information to support a device, it makes sense to broaden the scope by using the concept of "IoT product" to reflect an ecosystem-wide approach to IoT security. However, such expansion should be considered carefully in the context of this program.

[3] CSDE, International Anti-Botnet Guide. https://securingdigitaleconomy.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf

[4] CSDE, The C2 Consensus on IoT Device Security Baseline Capabilities. https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

A label should try to convey that other parts of the ecosystem – such as dependencies – are important as well for cybersecurity. However, that doesn't necessary mean that we need to include a great deal of information about back-end systems on the label that could potentially overwhelm the consumer. Instead, having transparency about the use of secure back-end systems might be a better approach than detailing the security information of those back-end systems.

However, when using a broader term such as "IoT product," it might become tricky in some cases to define the boundaries of a specific product, and certain components may well belong to more than one IoT product. ITI is committed to working with NIST to further refine the scope of the definition of IoT product and develop corresponding details of the labeling program.

- **We recommend NIST continue advocating for a consistent "IoT Device" definition in all *NISTIR* publications and with international partners to drive alignment in terminologies/terms.** While a view of security in the context of the larger ecosystem may be helpful, we recommend aligning the scope of NIST's security requirements to existing definitions that exclude conventional IT (as discussed below). Additionally, we recommend NIST explicitly spell out consistently within all NISTIR and IoT documents that IoT Devices are finished products, and that "components of a device, such as a processor or a sensor that transmits data to a purpose-built base station that cannot function at all on their own" should be out of scope of the document.[5] Consistent with NISTIR 8259, NIST should further clarify that general-purpose compute devices and conventional IT devices such as laptops and personal computers are distinct from IoT Devices and outside the scope here. Given the inclusion of a proposed new definition on "IoT Product" in this draft whitepaper, as mentioned above, ensuring alignment with terminologies/terms is critical to avoid inconsistency.

Caution Against Certification as a Comprehensive Solution

In terms of the conformity assessment approaches identified on page 10, ITI cautions against using certification as an approach because it is not a comprehensive solution for cybersecurity. Cybersecurity is not an end state. Rather, it is a continuous effort to protect products, services, and users, based on the latest threat/vulnerability information available using the best available techniques, throughout the deployment lifecycle. Because there is no one-size-fits-all solution to evaluate cybersecurity risks, certification cannot represent a complete picture of security or a "silver bullet solution." There are limited scenarios where certification could play a useful role: the product is suitable for certification (*e.g.,* an appropriate standard exists against which to certify), and a high level of assurance is required. In these limited cases, such assessments may provide a level of confidence to consumers and authorities. However, certification might not be appropriate for all products or use cases and governments should always consider alternatives to certification for managing cybersecurity risks.

Additionally, NIST has rightly pointed out in previous publications that multiple certification schemes for IoT products across jurisdictions and the lack of reciprocity between various types of certifications can fragment and drive up product costs. When deemed necessary based on risk, cybersecurity certification schemes should be grounded in international, industry-led, voluntary consensus standards and best

[5] NIST can clarify in a similar fashion to fn 2, at NISTIR 8259, p. 1, that "components are expected to be used along with other components to form an IoT device, but may play a role in the securability of an IoT device… [s]ince the focus of this publication is securability of the IoT device for the purposes of the customer [or consumer in this case], some or all of the concepts discussed may not apply to components". Compare to CSDE IoT Security Policy Principles at 3.

practices, such as the ISO/IEC 27000 series and the IEC 62443 suite of standards. Where appropriate, ITI encourages governments to reference such standards as written and published as the technical basis for certification schemes. Doing so will facilitate innovation and prevent the emergence of damaging technical barriers to trade (TBT). As referenced above, mandatory certification should be used only in situations where no better alternatives exist. In this context, flexibility is needed to apply vertical standards (*e.g.,* ISA/IEC 62443) that meet the horizontal baseline and extend beyond it. Finally, we note that NIST appropriately distinguished in a number of places between industrial, consumer and other use cases. As the work continues and additional standards and measures are considered, the distinction between the different use cases/verticals (and the difference between the needs and complexities associated with various intended audiences in the context of the measures) remains key.

Recognize Conformity Assessments by Suppliers/Vendors and Avoid Local Testing
NIST cites supplier declaration of conformity (SDoC) as one of the attestations (see p. 10), and ITI supports this recognition of conformity assessments by suppliers/vendors. In ITI's recently published policy principles for cybersecurity certification,[6] we strongly encourage governments to consider the viability of alternatives to certification, including education programs, voluntary standards, and first-party assessments. These alternative approaches to demonstrating compliance are used by vendors, are recognized and accepted by the marketplace, and are options with which industry has extensive experience. These approaches also respond to the need for flexibility, agility, and cost limits that must be borne by vendors (and, ultimately, purchasers). Examples of alternatives means of attestation include SDoC and vendor attestation.

In addition to recognizing supplier/vendor assessments, governments should also avoid localized testing and leverage mutual/multilateral recognition schemes. In particular, governments should leverage credible private-sector mutual/multilateral recognition schemes, such as the International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement, the International Accreditation Forum (IAF) Multilateral Recognition Arrangements (MLA), and the Common Criteria Recognition Arrangement (CCRA).

Ensure Labeling Conveys a Realistic Sense of Security and an Understanding of Shared Responsibility
NIST points out that labeling could be one confidence mechanism to provide end-users with clear information about companies' adherence to cybersecurity standards, as well as security features/functionality, to foster market competition. However, a label should not give the misleading impression that a product is completely secure. In ITI's recently published cybersecurity labeling position paper[7], we state that such an assumption would create a false sense of security and can serve to undercut the necessity for continuous improvement in cybersecurity practices. No label can possibly cover all vectors of attack, new vulnerabilities are continuously being identified, and labels are unlikely to cover the full range of security processes and activities manufacturers and end-users must take to maintain security.

In addition, any labeling proposal should communicate the policy objective, intended audience (such as consumer end-user, enterprise end-user, or regulator), objective criteria, and the conformity assurance process and associated labeling requirements as clearly as possible. Consumer awareness plays a key role, and we stress that cybersecurity is a shared responsibility, and manufacturers cannot secure the

[6] ITI Policy Principles for Cybersecurity Certification. September 2020.
[7] ITI Position Paper on Cybersecurity Labeling. April 2021.

products and services they develop without other stakeholders' participation. Both end-users and operators must understand their respective roles in maintaining cybersecurity.

Allow Flexible Label Formatting and Effective Content

A cybersecurity "label" should not only be conceived of as a physical sticker, especially in the digital space. The labeling scheme should be flexible to accommodate a range of formats, including electronic labeling (e-labeling) for digital listings in online marketplaces, machine-readable codes, and other forms of communication that effectively convey the security information to the intended audience. ITI recommends allowing the adoption of e-labels, a digital representation or an electronic means to display regulatory and other important information, which often provides links to an internet website or a scannable source. E-labeling is one potential way to convey information to end-users and regulators more effectively and efficiently than physical labels. We also encourage adopting the new ISO/IEC 22603 standard for e-labeling policy considerations.

In addition, we welcome the proposed tiered system approach on page 10 that is intended to reflect the increasing levels of cybersecurity. For the tiered approach to be useful and for the labels to be comparable, the tier structures must be the same, at least across an IoT product line, if not across all lines, if not across all lines, including general guidance for security best practices. For example, the lowest level self-attestation will have broad, positive impact, and is appropriate to many IoT products. Higher assurance testing should be used for critical systems, such as some medical devices and apps/services that manage highly sensitive data at scale.

In terms of how to convey cybersecurity with the tier structures to the consumer, it is important to highlight that labeling is only useful if it can be understood by the audience and provides information that can help them make decisions. For communication to be effective, any labeling scheme should streamline and simplify necessary information for the intended audience and avoid unnecessary information that may distract the consumer from understanding important security considerations. The consumer may even find sophisticated security information detail unhelpful or confusing, especially since this kind of information has generally not been available to inform consumer decisions in the past. Since this is a pilot program, we need to make sure whatever information we are providing is understandable and easy to read, perhaps in a standardized format that the consumer can digest.

Additionally, ITI recommends that any labeling program's process, costs, or related certifications should be clear, simple, and reasonable to avoid creating expensive, onerous obligations for manufacturers, which would discourage adoption. We recommend that policymakers consider conducting periodic reviews to assess the usefulness, effectiveness, and cost of cybersecurity labeling, as well as the impact of the labeling on improving security and end-users' decisions. Such assessments can help policymakers progress toward policy objectives, make needed adjustments, and better direct resources. We caution against any labeling requirements for unique, specialized, or local features that may create trade barriers or confusing information, and potentially burden companies by causing a fragmented approach to security labeling across different jurisdictions. We encourage policymakers to facilitate the mutual recognition of labeling, as well as third-party lab assessments, across jurisdictions as well. Doing so will help ensure prioritization of international standards-based programs, thus reducing fragmentation.

Conclusion

ITI has been pleased to respond to this public comment, and we would like to reiterate our industry's commitment to promoting global and domestic harmonization of IoT security proposals consistent with

core baseline capabilities for IoT security, driven by industry consensus and public-private collaboration, and grounded in global standards. We look forward to continuing to work with NIST and other USG stakeholders to maximize the benefits of IoT while mitigating risks using the best globally interoperable solutions.