CSDE

Council to Secure the Digital Economy

Non-Technical Criteria for Connected Device Security: Looking to the Long-Term

USTELECOM
THE BROADBAND ASSOCIATION

Consumer Technology Association

IN MAY 2021, the White House issued Executive Order 14028, *Improving the Nation's Cybersecurity*, which tasked National Institute of Standards and Technology (NIST), in coordination with the Federal Trade Commission (FTC) and other agencies, to initiate pilot programs for cybersecurity labeling, for consumer IoT, and for consumer software.

In February 2022, as part of their fulfillment of this directive, NIST published *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* (the "Criteria").[1] In developing the Criteria, NIST used existing work in IoT cybersecurity, including the NISTIR 8259 family of documents,[2] various industry standards, and an extensive stakeholder process that built on NIST work in this space.

The Criteria are not cybersecurity standards or "how to" design requirements. Rather they are the means by which one can assess whether a specific IoT cybersecurity label conformity assessment program (a label "scheme") has certain essential components, as defined by the Criteria. The Criteria can be used to evaluate the scheme's requirements for the IoT product, process for conformity assessment, and features of the resulting label. Some of the Criteria are technical in nature; some are non-technical.

The nature of the Criteria makes it difficult—even infeasible—to use the Criteria to directly assess an IoT product. As NIST writes, the goal of the Criteria document "…is to provide recommendations, additional information, and context related to these responsibilities for use by a scheme owner creating the consumer IoT product labeling program." In other words, the Criteria are to be applied to a scheme, not to a product.

As explained in the Criteria, *"NIST is identifying key elements of a potential labeling scheme that could be established by another organization or program…NIST is not establishing its own scheme or program, nor is NIST designing or proposing a design of a consumer IoT product label."*

To be effective, a cybersecurity labeling program for consumer IoT must include the following characteristics:

- Well-subscribed, industry-driven, and cost-effective cyber labeling in the U.S.
- Familiar and useful to consumers
- Maintained and administered
- Recognized in other regimes
- Systematic approach, traceable back to respected authorities
- Includes self-certification as an option for manufacturers
- Be formally recognized by federal and state governments as indicative of reasonable security

The overall framework that could emerge from the NIST work on consumer IoT labeling should not involve "compliance with NIST." This is clear from the goal stated in the Criteria; NIST is, as directed by EO 14028, establishing the means for verifying that a label scheme meets certain minimums.

Industry has existing IoT cybersecurity labeling programs. UL, Eurofins Digital Testing, CTIA, and others use voluntary industry consensus standards as the benchmark for conformity assessment. Going back to the checklist above, these programs can be utilized by manufacturers and advertised to consumers; they can be maintained and used as a basis for U.S. outreach to other regimes.

But are these programs "traceable back to respected authorities?"

The technical standards certainly are. A short list of specifications that have all had industry input are part of each program. However, the NIST Criteria evaluate the *non-technical* requirements of the label program as well.

Non-technical criteria are typical manufacturer practices that aren't observable properties of the devices. An observable property of the device might be, "encrypts data communications." On the other hand, it's not possible to review a product and observe what documentation was collected during its design.

Documentation, security query handling, and product education all fall under the heading of non-technical criteria. In fact, the NIST Criteria for consumer IoT labeling has these main categories:

Documentation: The IoT product developer creates, gathers, and stores information relevant to cybersecurity of the IoT product and its product components prior to customer purchase and throughout the development of a product and its subsequent lifecycle.

Information and Query Reception: The ability of the IoT product developer to receive information relevant to cybersecurity and respond to queries from the customer and others about information relevant to cybersecurity.

Information Dissemination: The IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the IoT product ecosystem) information relevant to cybersecurity.

Product Education and Awareness: The IoT product developer creates awareness of and educates customers and others in the IoT product ecosystem about cybersecurity-related information (e.g., considerations, features) related to the IoT product and its product components.

These categories are broadly stated and very inclusive, casting a wide net on all possibly useful sub-items in all cases. This is appropriate to the NIST Criteria, which seeks to cover all consumer IoT in all industry sectors and categories. What is needed next is refinement in a format similar to a technical standard—a "non-technical standard."

A technical standard has specific requirements that are amenable to verification; this verification is "conformity assessment." Such a non-technical standard would have parameters that bound each sub-item in the NIST list in a way that can be assessed by a third party, or can be internally verified in the case of self-attestation.

By way of example, the NIST technical criteria are mapped to and expressed in ANSI/CTA-2088-A. That consensus standard was derived from CSDE's "C2 Consensus." The Convene the Conveners (C2) project brought together the expertise of many technical experts via their various conveners: trade associations, standards development organizations, industry alliances, and coalitions. These groups shared and compared the expert recommendations each had developed within their own constituency. The work was coordinated under the auspices of CSDE and hosted by the Consumer Technology Association (CTA)®.

The mapping from the NIST Criteria to ANSI/CTA-2088-A isn't 1:1 because this is a sector-specific standard. However, the majority of NIST's all-inclusive (for a baseline) list of technical requirements is represented in the standard and in a measurable form.

Before we can see true compliance to the intent of the NIST Criteria, we need a similar *non-technical* standard, preferably an industry consensus document that brings in multiple stakeholders for the sector. In this way, just as the NIST technical criteria are supported by an industry technical standard, the NIST non-technical criteria will be supported by an industry non-technical standard.

Other gaps that will be discussed and filled over the next months include further work on sector-specific IoT (cybersecurity is different if you're looking at drones vs. doorbells), certain liability protections, a decision on whether a single national mark is appropriate, first steps toward international negotiation on mutual recognition, and education of consumers.

However, an important next step in this pipeline is to get the non-technical criteria standardized so that label scheme owners may consider how to adapt the industry consensus into their work.

ENDNOTES

1 https://doi.org/10.6028/NIST.CSWP.02042022-2

2 NIST, *NISTIR 8259 Series*, https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series