February 7, 2020

National Institute of Standards and Technology
Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899-2000

Re: NIST Request for Comment on NISTIR 8259 (Draft 2nd): Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline

I. Introduction

The Computing Technology Industry Association (CompTIA),[1] the leading association for the global information technology (IT) industry, appreciates the opportunity to provide comments to the National Institute of Standards and Technology (NIST) on NISTIR 8259 (Draft 2). CompTIA and its members are deeply committed to enhancing the resiliency of the connected ecosystem and we applaud NIST's valuable work to date in service of this goal. The Core Baseline capabilities for device manufacturers, now Table 1 of Draft 2, read in the context of the risk management approach articulated in NISTIR 8228,[2] provides a promising approach for increasing security across the IoT marketplace. We commend NIST on the Core Baseline and are optimistic that these documents will meaningfully advance the important goal of achieving a global core IoT security baseline.

We appreciate refinements made in Draft 2, particularly ongoing harmonization with the *C2 Consensus on IoT Device Security Baseline Capabilities*.[3] However, as discussed in CompTIA's comments on the previous draft, the Core Baseline must be more clearly distinguished from related guidance in order to be understood and used effectively.[4] While the Foundational Activities discussed throughout Draft 2 present valuable considerations, the Core Baseline itself is the product of widespread stakeholder consensus and outlines technically verifiable capabilities. Though CompTIA does not support codification of these evolving technical capabilities into legislation or regulation itself, NIST should prepare for the document's potential use by a regulator, policymaker, or court. Therefore, we urge NIST to publish the Core Baseline separately from the rest of Draft 2 and instead incorporate the Core Baseline by

---

[1] CompTIA supports policies that enable the information technology industry to thrive in the global marketplace. We work to promote investment and innovation, market access, robust cybersecurity solutions, commonsense privacy policies, streamlined procurement, and a skilled IT workforce. Visit www.comptia.org to learn more.
[2] National Institute of Standards and Technology, *NISTIR 8228: Considerations for Managing the Internet of Things (IoT) Cybersecurity and Privacy Risks* (June 2019).
[3] *The C2 Consensus on IoT Device Security Baseline Capabilities*, Council to Secure the Digital Economy (September 2019), https://securingdigitaleconomy.org/projects/c2-consensus/.
[4] CompTIA Comments on *NISTIR 8259 (Draft): Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for Manufacturers* (Sept. 30, 2019), https://comptiacdn.azureedge.net/webcontent/docs/default-source/advocacy-documents/comptia-nistir-8259-comments-(9-30-19).pdf?sfvrsn=28b2e7da_2.

reference into the final NISTIR 8259. Such an approach will encourage manufacturers to adopt the core baseline while allowing stakeholders to continue discussion on related best practices.

With this in mind, CompTIA respectfully submits these comments and looks forward to continued collaboration with NIST and our fellow stakeholders.

II. The Baseline Must Be More Clearly Distinguished from Related Guidance that is Not Baseline.

As noted in previous comments by CompTIA and other stakeholders, the Core Baseline represents a distinct set of consensus-based, technically verifiable capabilities and should be clearly distinguished from NIST's related IoT guidance. While Draft 2 provides some helpful refinement to the earlier version of NISTIR 8259, it now includes the Core Device Cybersecurity Baseline within a "Foundational Activity," which provides less distinction than the first draft and reduces the visibility of the Core Baseline itself. Rooted in the ongoing work of more than a dozen IoT device security guidance documents published by standard-setting bodies, associations, and government agencies, the Core Baseline is fundamentally more deeply grounded in broad stakeholder consensus than the rest of NISTIR 8259, which, while valuable, is a matter of ongoing discussion.

Placing the Core Baseline within a Foundational Activity not only mischaracterizes the significance of the consensus that the Core Baseline carries with it, but would functionally weaken the impact of the Core Baseline in the marketplace. Although the Foundational Activities are helpfully framed as questions for manufacturers to consider, the Core Baseline itself should function as described in footnote 3, as "a set of foundational requirements or recommendations."[5] By conjoining the Core Baseline with open-ended considerations, Draft 2 creates a disincentive for manufacturers to explicitly adopt and rely on the Core Baseline for fear of inadvertently assuming liability. While the Foundational Activities in Draft 2 provide valuable considerations for manufacturers to discuss, the Core Baseline is something to which a manufacturer can measurably attest. It functions differently, and therefore should be presented distinctly.

III. NIST Should Publish the Core Baseline Separately from Discussion of Foundational Activities.

NIST should prepare for the document's potential use by a regulator, a policymaker, or a court – and should do so by publishing the Core Baseline as a standalone document. While codifying evolving technical capabilities into legislation or regulation itself would be highly problematic, it is possible, even likely, that state and federal policymakers will look to NIST for guidance on what constitutes reasonable security measures by IoT device manufacturers. Previously, for example, the state of Ohio chose to incorporate several NIST publications as a "safe harbor" in its 2018 Data Protection Act.[6] In that Act, Ohio provides a legal safe harbor to covered entities with cybersecurity programs that reasonably conform to the current version of the "'framework for improving critical infrastructure cybersecurity' developed by the 'national institute of standards and technology'" or "NIST special publication 800-171" or "NIST special

[5] Draft 2 at 11, n.3.

[6] Ohio Data Protection Act, 2018 SB 220, https://www.legislature.ohio.gov/legislation/legislation-documents?id=GA132-SB-220.

publications 800-53 and 800-53a." Notably, the law refers to these documents as a whole, not to a specific section or table contained within. In refining Draft 2, NIST should keep in mind the likelihood that a similar reference might be made in IoT device legislation. As currently drafted, NISTIR 8259 would conflate verifiable technical capabilities with open-ended questions for consideration. To address this issue and provide clarity in how best to use and understand NIST's IoT security guidance, NIST should publish the Core Baseline as a standalone document and incorporate it by reference into the rest of NISTIR 8259.

IV. Conclusion

CompTIA appreciates the opportunity to provide comments on NISTIR 8259 Draft 2. We commend NIST on its valuable work in advancing IoT security. In continuing to refine NISTIR 8259, we urge NIST to publish the Core Baseline as a standalone document to provide clarity for users and facilitate widespread adoption of this guidance. Harmonized, effective global IoT security practices are vital in our increasingly connected ecosystem and CompTIA and its members look forward to continued work with NIST in service of that goal.

Respectfully submitted,

/s/ Savannah P. Schaefer

Savannah P. Schaefer
Senior Director, Public Advocacy
CompTIA
322 4th Street, NE
Washington, DC 20002