September 30, 2019

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Connecticut Ave., NW
Washington, DC 20230

Re: NIST Request for Comment on NISTIR 8259 (Draft): Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers

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 in response to the above-captioned request for comments. CompTIA's membership spans a wide range of the connected ecosystem. From manufacturers of IoT devices and components to the IT hardware, software, and services providers that connect them to the security services providers that manage and mitigate risks associated with IoT devices, CompTIA represents industry members dedicated to increasing security across the IoT marketplace to enhance the resiliency of global communications networks.

CompTIA deeply appreciates the National Institute of Standards and Technology's (NIST's) commitment to stakeholder-driven processes. We applaud NIST's thoughtful, risk-based approach to enhancing IoT security as outlined in NISTIR 8228 and supported by the "Core Baseline for IoT Devices" in Section 4 (the Baseline) of Draft NISTIR 8259 (the Draft).[2] We agree that to be understood appropriately and used effectively the Baseline must be read in the context of NISTIR 8228 and view the background synopsis on the prerequisite document as highly valuable. Similarly, to clarify the roles and relationships of these documents, the Baseline should be distinguished from related guidance in Sections 3, 5, 6, and 7 of the Draft that is valuable but not baseline itself. Additionally, NIST should clarify that the Draft's guidance applies to finished IoT products, not individual components of an IoT device that cannot function without being imbedded or integrated into a product. Furthermore, we suggest NIST clarify language regarding device identification to convey the distinct role of identification for IoT apart from traditional IT.

Alongside more than twenty other organizations – collectively representing thousands of stakeholder companies – CompTIA participated in the C2 effort that produced the *C2 Consensus*

[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, *Considerations for Managing the Internet of Things (IoT) Cybersecurity and Privacy Risks (NISTIR 8228)* (June 2019).

on IoT Security Baseline Capabilities (the C2 Consensus).[3] We strongly support both the C2 Consensus and NISTIR 8259 as aligned efforts that accurately reflect what may be deemed reasonable IoT capabilities today and tee up a clear vision for how to enhance these capabilities going forward. As NIST looks toward next steps, we suggest the agency work with stakeholders to map the Baseline to the C2 Consensus for clarification on where further alignment may be necessary and how the documents can best be used together. Reducing regulatory fragmentation is key to bolstering security across the IoT marketplace, and we are confident these efforts will provide a strong foundation for harmonization of IoT device security expectations internationally, enabling efficiencies of scale and clarity regarding shared risk management responsibilities.

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

II. CompTIA Suppots Draft NISTIR 8259 and NISTIR 8228 as a Starting Point for IoT Device Manufacturers.

As part of ongoing efforts across the Departments of Commerce, Homeland Security and other federal agencies to enhance resiliency of the information and communications technology (ICT) ecosystem, CompTIA commends NIST on the open and collaborative approach taken to develop the Baseline and related guidance. The Baseline demonstrates the value of strong partnership, benefitting from NIST's technical expertise and convening capacity and leveraging the broad range of experience across its many stakeholders. Recognizing the diverse world of IoT products, NISTIR 8228 and Draft NISTIR 8259 appropriately frame minimum cybersecurity capabilities in the context of an overall risk management process wherein a given IoT device will need different security capabilities and configuration depending on the individual risk environment in which it operates.

With the exponential proliferation of IoT devices and as new use cases for this technology emerge, coalescence around a global core baseline for IoT devices is vital. Draft NISTIR 8259 is a strong starting point in this effort. As NIST works to refine the core Baseline, CompTIA strongly supports further alignment with key efforts like the C2 Consensus in order to foster as widespread use as possible.

III. The Baseline Should Be Distinguished from Related Guidance that is Not Baseline.

As stated above, CompTIA strongly supports development of a core IoT cybersecurity baseline and views Section 4 of Draft NISTIR 8259 as material advancement toward this goal. However, in order for the Baseline in Section 4 to be understood and used effectively, it should be distinguished from related guidance in Sections 3, 5, 6, and 7. Though each of these sections provide valuable insight for manufacturers on customer use case considerations, feature implementation, communicating cybersecurity information to customers, and secure development practices, unlike Section 4 they do not present technically verifiable capabilities.

[3] *The C2 Consensus on IoT Device Security Baseline Capabilities*, Council to Secure the Digital Economy (September 2019), https://securingdigitaleconomy.org/projects/c2-consensus/.

Furthermore, aspects of Sections 3, 5, 6, and 7 remain subject to debate among stakeholders and merit additional discussion beyond the scope of the Baseline itself. To avoid stakeholder confusion, misapplication, and to foster widespread adoption of the Baseline, NIST should place related guidance that is not baseline in a separate document.

IV. NIST Should Clarify the Distinction Between Components and Finished Products.

To further facilitate use and avoid misapplication of the Baseline, NIST should clarify that the guidance offered in the Draft applies to finished IoT products, not components. Throughout the Draft, NIST is clear that the Baseline and related guidance are developed for "IoT devices." However, given broad ongoing discussion about how to define IoT, NIST should clarify that "device" refers to a finished product available to consumers which is usable for its intended functions without being imbedded or integrated into any other product. Conversely, the Draft's guidance does not apply to a component, which is a physical object that is not usable for its intended functions without being imbedded or integrated into any other product. This distinction has been recognized in statute, for example in the context of sanctions law,[4] and is valuable in this context for similar reasons. The security capabilities outlined in the Baseline are features that a device itself could be expected to achieve but would not make sense to expect from each component of that device. Including this distinction in the Draft will provide clarity for device manufacturers and help policymakers more clearly understand how the Baseline is used.

V. NIST Should Clarify the Distinct Role of Device Identification for IoT.

In NISTIR 8228 and reiterated in the background of Draft NISTIR 8259, NIST appropriately recognizes that many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can. This presents different challenges for managing IoT assets since IoT devices often do not have the same capacity for running clients or software to scan for malware or vulnerabilities as their conventional IT counterparts. Just as NIST recognizes that IoT devices operate differently than IT devices in many cases, the Baseline should clearly recognize that client or agent-based mechanisms to secure conventional IT may not work equivalently in the IoT context because installing clients, agent or endpoint software may not be technically feasible. For accurate asset management and device visibility, devices should be capable of being identified without the need for a client to be installed at the IoT endpoint. To that end, we suggest clarifying this principle for IoT device identification in the rationale section in Table 1.[5]

VI. The Baseline Should Be Mapped to the C2 Consensus.

As mentioned, CompTIA joined fellow trade associations, standard setting organizations, and industry alliances in development of the C2 Consensus earlier this year. We support both the C2 Consensus and the Baseline as leading efforts to facilitate global alignment around a core cybersecurity baseline. As NIST works to refine Draft NISTIR 8259, we encourage NIST to

[4] See 50 U.S.C. § 4611.

[5] *See* National Institute of Standards and Technology, *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers (Draft NISTIR 8259)* (July 2019) at 10.

work with the C2 Consensus participants to understand where the respective baselines differ and how best to align them moving forward. To enhance security of the IoT marketplace and overall ICT ecosystem, stakeholders need broad engagement and agreement across industry, government, and internationally. Aligning the C2 Consensus with the Baseline provides a key next step toward this goal.

VII. Conclusion

CompTIA appreciates the opportunity to provide comments on Draft NISTIR 8259. We commend NIST on the Baseline, which represents the product of widespread collaboration among expert stakeholders. As NIST works to refine the Draft, we suggest the clarifications above to facilitate effective and widespread adoption of this guidance. Alongside the C2 Consensus, this Baseline advances the goal of achieving a global core cybersecurity baseline for IoT. We look forward to continued work with NIST to meet this goal in pursuit of an increasingly resilient ICT ecosystem.

Respectfully submitted,

/s/ Savannah P. Schaefer

Savannah P. Schaefer
Senior Director, Public Advocacy
COMPTIA
515 2nd Street NE
Washington, DC 20002

September 30, 2019