October 24, 2018

Via Electronic Filing (iotsecurity@nist.gov)

Re: Comments of the Telecommunications Industry Association to the National Institute of Standards and Technology on the *Draft NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks.*

I. INTRODUCTION

The Telecommunications Industry Association ("TIA") respectfully submits these comments in response to the Draft National Institute of Standards and Technology's ("NIST") Interagency Report ("IR") 8228 Considerations for Managing IoT Cybersecurity and Privacy Risks ("Report").[1]

As both a standard setting body and advocacy organization, TIA represents hundreds of manufacturers and vendors of information and communications technology ("ICT") equipment and services supplied to critical infrastructure owners and operators across the globe, enabling secure and resilient network operations across myriad segments of the economy.[2] Over the last year, TIA and many of its members have participated in NIST's "listening sessions" to provide input on the development of this Report, including the workshop held at NIST's campus in Gaithersburg last July. TIA appreciates NIST's continued work to provide tools for federal agencies to improve their cybersecurity posture as well as NIST's commitment to transparent, collaborative partnership with industry and other stakeholders throughout this process.

The increasing proliferation of connected devices is transforming the ways we live and operate, presenting vast potential benefits as well as new challenges for security and privacy. TIA commends NIST for developing this detailed Report at such an important time. As the Report correctly recognizes, "[b]ecause IoT devices and their uses and needs are so varied, few recommendations can be made that apply to *all* IoT devices."[3] Consistent with this understanding, NIST outlines helpful considerations regarding IoT cybersecurity and privacy risks as well as mitigation challenges associated with those risks. Additionally, the Report provides a helpful process for organizations to begin to understand and manage those risks with respect to their own IoT devices, consistent with established cybersecurity risk management approaches. Appendix A provides a useful collection of potential IoT capabilities and tangibly shows how this collection of capabilities could provide a starting point for organizations to

[1] National Institute of Standards and Technology, Draft NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, publ. Sept. 24, 2018.

[2] Additionally, TIA writes and maintains voluntary industry standards and specifications, as well as formulates technical positions for presentation on behalf of the United States in certain international standards fora. TIA is accredited by the American National Standards Institute (ANSI) to develop voluntary industry standards for a wide variety of telecommunications products and sponsors more than 70 standards formulating committees. These committees are made up of over 1,000 volunteer participants, including representatives from manufacturers of telecommunications equipment, service providers, and end-users – including the United States government. Member companies and other stakeholders participating in the efforts of these committees and sub-groups have produced more than 3,000 standards and technical papers that are used by companies and governments to produce interoperable products around the world.

[3] Report at viii, emphasis added.

analyze and assess baseline capabilities for a particular IoT device based on the organization's situational needs.

In framing these recommendations and potential capabilities for IoT devices, however, NIST should refine some language to more clearly reflect the Report's risk management approach. NIST must remain clear throughout the document and in communicating this guidance more broadly that proposed "baselines" do not apply "universally" to every device or every implementation. While TIA agrees that "more specific and actionable recommendations can be made for particular types of IoT devices," TIA urges NIST to provide greater clarity that the guidance in this Report should be viewed as part of an ongoing risk management process wherein the security requirements of a device are determined in the context of its function and configuration in the network.

Once final, TIA believes this Report will provide a valuable foundation for understanding cybersecurity and privacy risks associated with IoT. TIA offers a few high-level comments below and looks forward to continued work with NIST and its stakeholders to finalize this publication.

II. TIA SUPPORTS THE RISK MANAGEMENT PROCESS ARTICULATED IN THIS REPORT

Consistent with seminal cybersecurity risk management tools like the Framework for Improving Critical Infrastructure Cybersecurity,[4] Draft NISTIR 8228 proposes a flexible, risk-based approach for federal agencies to identify and manage risks associated with IoT devices throughout their lifecycles. This approach, as summarized in Section 5 "Recommendations for Addressing Cybersecurity and Privacy Risk Mitigation Challenges for IoT Devices," outlines a process wherein organizations must 1) understand risk considerations and mitigation challenges, 2) adjust organizational policies and processes accordingly, and 3) implement updated mitigation practices.[5] Figure 7 helpfully elaborates how an organization might "start with a list of capabilities and filter them *within the context and risk of a particular situation*—a certain type of IoT device being deployed in a particular environment for a stated purpose."[6] Appendix A goes on to note that "[t]his reflects that in many cases, not all capabilities will be applicable."[7] TIA supports this sort of approach, focused on promoting risk management choices informed by the context in which the IoT device is deployed.

III. TIA SUPPORTS REFINEMENT OF LANGUAGE REGARDING POTENTIAL IOT SECURITY AND PRIVACY CAPABILITIES

While TIA supports this Report's overall risk management approach, some language, like that articulating potential "baseline" capabilities or "universal" recommendations could be refined to more clearly reflect that approach. As this guidance is communicated to broader audiences, common connotations of the terms used will be increasingly important. To promote informed, effective risk management and prevent ossification of this Report's guidance into a compliance checklist, NIST should more clearly define what is meant by the "high-level, widely applicable baseline" it aims to provide as opposed to the "baselines and recommendations for particular IoT device types" it intends to develop.

---

[4] Framework for Improving Critical Infrastructure Cybersecurity, see cyberframework@nist.org.
[5] Draft NISTIR 8228 at 25.
[6] *Id.* at 29, emphasis added.
[7] *Id.*

NIST should also consider whether "universal" is an appropriate way to describe recommendations offered in this Report.

As NIST notes, "[t]he term 'baseline' has different meanings to different people and organizations."[8] In this Report, NIST aims to create a "high-level, widely applicable baseline" for IoT device risk mitigation and explains in footnote that the term "baseline" is used here "in the generic sense of a set of requirements or recommendations."[9] It goes on to say the "first examples" of this "high-level baseline" are "shown in Appendix A." While Figure 7 demonstrates that the "examples of possible cybersecurity and privacy capabilities" articulated in Appendix A must be filtered "within the context and risk of a particular situation," the term "baseline" could yet be misconstrued to imply that these capabilities should instead extend to all IoT devices.[10] Though the recommended risk management approach in this Report makes clear that NIST does not intend to create a one-size-fits-all IoT security and privacy checklist, NIST should clarify this further by elaborating on its definition of "baseline" or considering whether another term in some areas might more accurately reflect its intention.

Similarly, use of the term "universal" may confuse readers in this Report. In the Executive Summary, NIST states "[b]ecause IoT devices and their uses and needs are so varied, few recommendations can be made that apply to all IoT devices; Appendix A provides examples of possible universal recommendations."[11] While Section 5 articulates a broadly applicable approach to IoT cybersecurity risk management, no portion of this Report proposes a specific recommendation applicable to every device or every organization, without limit or exception. Nor should it; such a recommendation would most likely be inaccurate or so broad as to be unhelpful. This Report takes the right approach by recommending a risk management process, articulating possible challenges and capabilities, and proposing that more specific and actionable recommendations be made for specific use cases. Language describing the scope and content of Appendix A should be refined for consistency with that approach.

IV. CONCLUSION

TIA thanks NIST for its public request for stakeholder input on Draft NISTIR 8228. As NIST works to refine this Report, we look forward to continued collaboration with NIST and its stakeholders on this important work.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: */s/ Savannah P. Schaefer*

Savannah P. Schaefer
Policy Counsel, Government Affairs

[8] *Id.* at vii, n. 2.
[9] *Id.* at iv.
[10] *Id.* at 29.
[11] *Id.* at vi.