April 18, 2018

National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

VIA EMAIL: NISTIR-8200@nist.gov

RE: ITI Comments to NISTIR 8200 – "Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)"

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to the National Institute of Standards and Technology's (NIST's) draft Interagency Report (NISTIR) 8200, *Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)* (hereinafter, "the Report").

ITI, the global voice of the tech sector, 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. ITI has long commended NIST's work in partnering with the private sector and other stakeholders to further the development and use of voluntary standards and frameworks to manage cybersecurity risks. ITI continues to support the Interagency International Cybersecurity Standardization Working Group (IICS WG) in fulfilling its purpose to coordinate on major issues in international cybersecurity standardization, thereby enhancing U.S. federal agency participation in international cybersecurity standardization efforts. We thank NIST and the IICS WG for their acknowledgement of the contributions of the private sector in standards development in the United States.

As the Report identifies, the growth of network-connected devices, systems, and services comprising IoT creates immense opportunities and benefits for our society. To reap the great benefits of IoT and to minimize the potentially significant risks, these networked connected devices need to be secure and resilient. We agree that achieving greater security and resilience depends in large part upon the timely availability and widespread adoption of clear and effective international cybersecurity standards. We appreciate that the Report's approach is not heavy-handed and did not attempt to endorse a particular definition of IoT. We commend NIST and the Internet of Things Task Group for undertaking this significant and helpful effort to lay out the current state of international cybersecurity standards development for IoT and would like to offer the following recommendations to NIST to help build on the draft Report,

which we believe can serve as a starting point to organize identified standards around a framework approach in the future.

1. **The Report should further clarify its purpose and intended use.**

While we understand that the IICS WG member agencies plan to "look to this report to assist them in their standards planning and to help to coordinate U.S. government participation in international cybersecurity standardization for IoT"(p. ii), we believe it is important that NIST explain early on how this Report will relate to or feed into similar and parallel efforts being pursued by other groups across the USG. In particular, we ask that NIST clarify the overall USG approach towards the IoT and how it differs from its approach to industrial control systems. Additionally, we believe it would be helpful for NIST to explain how this Report interplays with current draft IoT frameworks. If possible, we recommend that these efforts be more coordinated across the USG.

2. **Further build out how "standards gaps" would be addressed.**

We believe that this Report can be an informative repository helpful in mapping IoT security standards development, but we are concerned that in its current form, it draws conclusions or implies potential action items that are not fully fleshed out. For example, while the Report identifies a set of "standards gaps" (Clause 10), there is scarce detail on how addressing such gaps would meet market needs and gain adoption. We believe these matters deserve more attention to meaningfully contextualize the substantial annexes at the end of the document.

3. **The "Cybersecurity Objectives" exclude important elements**

While the "cybersecurity objectives"(p. 33) for IoT systems as identified in the Report include "Confidentiality, Integrity and Availability," this section overlooks some of the major issues related to hacking of such systems that enables them to be taken over for malicious purposes, or cases where connections from IoT systems can be hijacked for nefarious purposes. These incidents don't neatly fit into the Confidentiality, Integrity and Availability paradigm and these areas are the major difference in focus between "cybersecurity" and classic "information security." The Report should emphasize the centrality of systems and subsystems rather than "information" in its cybersecurity objectives. We appreciated the Report's reference to "trustworthiness" (p. 33) in addition to "cybersecurity" as a goal since there are other major aspects of IoT systems that also need to be addressed in addition to security - such as safety. We recommend more heavily emphasizing trustworthiness throughout the document rather than just in the beginning of this section.

4. **Emphasize use of industry standards for government procurement**

We support the Report's conclusion that "the availability and use of international cybersecurity standards are major factors for ensuring the secure and resilient operation of the expanding number of agency mission critical IoT systems" (p. 56) and that in accordance with USG policy,

agencies should support the development of appropriate conformity assessment schemes to the requirements in such standards. We believe, however, that the Report should also highlight the importance of government procurement policies allowing use of industry standards rather than separate government standards where possible for cyber and supply chain security. Companies which have conformed their internal processes to an international standard should not be required to certify separately for government procurement.

5. **Maintain an international perspective.**

Given the intended audience of the Report is both the government and public and the express purpose "is to inform and enable policymakers, managers, and standards participants as they seek timely development of and use of such standards in IoT components, systems, and services" (p. iii) it is likely that other governments will look to the Report and corresponding list of standards as a model for their own IoT cybersecurity standardization schemes. For this reason, it is important that NIST's efforts are carefully contextualized and it is clarified up front how this report will be used to further industry-led, voluntary standards-based approaches. We believe this Report could become an important tool to promote interoperable standards in various international markets including, but not limited to, the EU, China, Japan, and India.

Conclusion

ITI would like to thank NIST for its commitment to partnering with the private sector to advance our shared goals to advance cybersecurity standardization and IoT security. NIST's ongoing commitment to industry outreach is an excellent example of how effective public-private partnership processes can help to improve cybersecurity. ITI and our members look forward to continuing to work with NIST, the Administration and international stakeholders to build on the solid foundation established by the Report to further international cybersecurity standardization efforts for IoT, as well as other initiatives to improve our cybersecurity posture. Please continue to consider ITI as a resource on cybersecurity issues, and do not hesitate to contact us with any questions regarding this submission.

Best Regards,

John Miller
Vice President for Global Policy and Law