Coalition for Cybersecurity Policy & Law

Coalition for Cybersecurity Policy & Law
600 Massachusetts Ave, NW, Washington, DC 20001

April 17, 2018

VIA EMAIL: NISTIR-8200@nist.gov

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

Re: Comments of the Coalition for Cybersecurity Policy & Law

The Coalition for Cybersecurity Policy & Law ("Coalition") submits this comment in response to the Request for Comments ("RFC") issued by the National Institute of Standards and Technology ("NIST") on February 14, 2018.[1] The RFC seeks input on the draft Interagency Report on [the] Status of International Cybersecurity Standardization for the Internet of Things (Report).[2] The Coalition supports NIST's efforts to promote and facilitate the development of appropriate standards in the Internet of Things ("IoT") environment. The Report provides a helpful resource to aid organizations in identifying existing standards for IoT devices. It also provides a useful starting point for further coordination amongst public and private sector organizations to develop robust standards that address the specific security issues presented by IoT applications. The Coalition appreciates the opportunity to provide input on the Report and to participate in the process of identifying and developing standards that work for all types of IoT applications.

The Coalition is comprised of leading companies with a specialty in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[3] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management, and we are supportive of efforts to identify and promote the adoption of cybersecurity best practices and voluntary standards throughout the global community.

[1] NIST, Draft Interagency Report, NISTIR 8200, Summarizes International Efforts to Standardize Internet of Things Cybersecurity, https://csrc.nist.gov/News/2018/Report-International-IoT-Cybersecurity-Standards.
[2] NIST, Interagency Report on [the] Status of International Cybersecurity Standardization for the Internet of Things (IoT), https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf. ("Report")
[3] The views expressed in this comment reflect the consensus view of the Coalition and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, *see* www.cybersecuritycoalition.org.

I. The Report Provides Useful Guidance on Existing Security Standards and Facilitates Further Standards Development

The Coalition's Membership has been at the forefront of the standards development process for decades, working with government agencies, standards development organizations, and industry groups to identify and promote best practices and robust standards in cybersecurity. These standards form a common security baseline that makes the entire online ecosystem more secure. The Coalition agrees that the development and adoption of appropriate security standards is essential to the resilience and continued growth of the market for IoT devices. The Report facilitates this effort by cataloging the existing security standards that organizations should consider implementing, if they have not already done so. The Report also identifies the availability of and the extent to which existing standards have been implemented in Table 4, which identifies whether standards are available across the core areas of cybersecurity for each of the example IoT applications identified in the Report.[4] This table is particularly helpful in identifying areas in need of further standards development work.

The Coalition also supports NIST's efforts to provide greater clarity about the terminology used to describe IoT devices and the capabilities of such devices. The development of common standards requires that the relevant parties have a common framework for discussing the security needs and device capabilities in IoT applications. The Report provides a common reference point that can be used to facilitate such discussions. Establishing a common framework for discussions about IoT security can be particularly difficult because the IoT ecosystem is continuing to develop and already includes a wide variety of applications in the marketplace with varying capabilities and features.

The Coalition further agrees that the development of appropriate IoT security standards requires a common understanding of the objectives of such standards, the threats faced by IoT applications, and the risks these threats pose to the confidentiality, integrity, and availability of the information processed by various IoT applications. The Coalition believes that NIST's adaptation in the Report of the security objectives identified in NIST SP 800-82 to the IoT ecosystem establishes a useful reference point to identify the goals that security standards should promote.[5] Some of these objectives can be particularly important in IoT applications, such as preventing the unauthorized modification of data and maintaining functionality during adverse conditions, as security failures in some IoT applications can have a physical impact on the health and safety of the users of those applications.

The Coalition also finds the section of the Report that identifies objectives, risks, and threats across several examples of IoT applications to be a helpful illustration of how organizations should consider these issues when setting standards for the IoT ecosystem.[6] In particular, these examples highlight the variety of unique risks and threats that are faced by different IoT applications. The chart identifying the risks to network medical devices and

[4] *Report* at 53.
[5] *Id.* at 35.
[6] *Id.* at 36-45.

connected ID networks is particularly helpful, and the Coalition encourages NIST to consider including a similar table for each of the example IoT applications.

II. The Coalition Recommends that NIST Consider Certain Modifications to the Report to Provide Greater Clarity

The Coalition broadly supports the work NIST has done in preparing the Report and suggests the following revisions to help clarify the Report's important message. The Coalition encourages NIST to make a substantive revision to the description of the Internet of Things in section 4, as well as several organizational edits throughout the Report. We identify these edits below and in the attached appendix, which uses the comment template provided with the RFC.

Description of IoT. The Coalition believes that the Report's description of IoT is overly broad. The Report states that the Internet of Things consists of components that are connected by a network providing the potential for a many-to-many relationship between components and some of the IoT components have sensors or actuators that allow for interaction with the physical world.[7] The Report describes a component as an entity that can interact with other entities to form systems that can achieve goals.[8] The Report also describes IoT as "a concept based on creating systems that interact with the physical world using networked entities (e.g. sensors, actuators, information resources, people)."[9] Because a consensus definition of IoT has not yet emerged from the efforts of various standards organizations, industry participants, and governmental bodies and because any such definition would need to address a wide variety of IoT applications with differing functionalities, capabilities, and complexity, the Coalition encourages NIST to map to existing descriptions of IoT throughout the Report rather than proposing its own description. This will allow the Report to reflect the variety of descriptions that have been put forth and allow for a more targeted discussion of IoT standards that are specific to the various IoT applications that exist in the marketplace.

Reclassification of the Network Interface Capability. The Coalition encourages NIST to reclassify the "network interface" capability as a primary capability of an IoT component. The Report identifies the network interface capability as a secondary capability but states that "[e]very IoT component must have at least one network interface capability…."[10] Since the network interface capability is a required function of all IoT components, the Coalition believes that it would be more appropriate to identify it as a primary capability.

IoT Examples. The Coalition encourages NIST to consider revising the examples of IoT applications that are discussed in section 5 of the Report. Specifically, the Coalition encourages NIST to broaden the examples and discuss them generally rather than discussing the examples by identifying specific types of IoT devices, such as smart light bulbs or sous vide machines. The current examples appear as if they are an attempt to identify categories of IoT applications, particularly when used in section 7 to discuss the objectives, risks, and threats specific to each

[7] *Id.* at 4.
[8] *Id.*
[9] *Id.*
[10] *Id.* at 8.

example.[11] To the extent they are intended to establish categories of IoT applications, they do not clearly identify the scope of the categories they are intended to establish. For example, the Report does not clearly identify whether "Consumer IoT" covers consumer IoT devices when used for business purposes.[12] The examples also do not address uses of IoT devices in the transportation field outside of connected vehicles, nor do they address the use of IoT devices by municipalities for infrastructure or other purposes. The Coalition also believes that the "Smart Building" example is over-inclusive, as it could be understood to include smart home devices, which are more appropriately viewed as consumer devices, and the "Smart Manufacturing" example is under-inclusive because it does not capture the variety of use cases for which businesses employ IoT devices.

To clarify the scope of the examples and make them more useful as categories of IoT applications, the Coalition encourages NIST to make the following changes: (1) revising the "Consumer IoT" example to "Smart Devices"; (2) revising "Smart Manufacturing" to "Commercial IoT"; (3) revising "Smart Building IoT" to "Smart Office IoT"; and (4) clearly stating that municipal uses of IoT should be considered to fall within the Industrial IoT example. These changes will require some revisions in the sections discussing each examples, and the Coalition encourages NIST to use this opportunity to discuss each example more broadly, identifying the common elements and the unique considerations of each type of IoT application.

Connected Vehicle Cybersecurity Objectives. The Coalition suggests that the chart identifying the cybersecurity objectives for connected vehicles be updated to include encryption of data at rest. The chart provides a useful resource, and it already identifies the need for encryption to protect the confidentiality of information transmitted by connected vehicles; however, it does not indicate that such information should also be encrypted at rest. Adding such a statement to the chart will highlight the need to ensure that this data is protected against attack at all times.

Description of Cybersecurity Risks for Medical Devices. The Coalition recommends that NIST adapt Table 3 from the report describing the risks for health IoT and medical devices, for each of the IoT applications identified in the Report. This table is a useful way to present this information and would help readers understand the risks for each of the other IoT applications discussed in the Report.

Standards Landscape for IoT Cybersecurity. At the beginning of Section 8, the Report includes a list of important considerations for securing IoT applications. The Coalition views this list as setting out foundational considerations for any discussion of IoT security and encourages NIST to move the list to its discussion of the Internet of Things in Section 4. Moving this list earlier in the Report will emphasize its importance and will provide readers with necessary background to help them better understand the remainder of the Report.

[11] *Id.* at 33-45.
[12] *Id.* at 10.

III. Conclusion

The Coalition thanks NIST for its leadership in this important effort. We value the opportunity to participate in this discussion by commenting on the Report. We look forward to continuing to work with NIST on efforts to improve IoT cybersecurity.

Comment Template for Draft NIST Interagency Report (NISTIR) 8200 -- Status of International Cybersecurity Standardization for the Internet of Things (IoT)

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1	The Coalition for Cybersecurity Policy & Law	Major	Lines 317-340 Page 4	The current description of IoT is overly broad. The Report would better reflect the variety of proposed descriptions that have been put forth and allow for a more targeted discussion of IoT standards that account for the variety of IoT applications that exist in the marketplace if it maps to existing descriptions of IoT.	The Coalition encourages NIST to map to existing descriptions of IoT throughout the Report rather than proposing its own description of IoT.
2	The Coalition for Cybersecurity Policy & Law	Minor	Lines 434-441 Page 8	The Report currently states that the network interface capability is a secondary capability; however, it also states that every IoT component must have at least one network interface capability. Since all IoT components must have this capability, the Coalition believes that it should be identified as a primary capability.	The Coalition recommends that NIST reclassify the network interface capability as a primary capability.
3	The Coalition for Cybersecurity Policy & Law	Major	Lines 463 – 760 Pages 9 - 21	The examples identified in section 5 currently do not address commercial IoT applications outside of the context of smart buildings and smart manufacturing. The examples also do not address the use of consumer IoT applications for business purposes or how to classify smart home IoT applications. The examples also do not provide guidance on how to classify municipal IoT applications.	The Coalition encourages NIST to consider revising the examples of IoT applications that are discussed in section 5 of the Report to broaden the examples and address them generally.
4	The Coalition for Cybersecurity Policy & Law	Minor	Line 1385 Page 37	The chart identifying cybersecurity objectives for connected vehicles identifies encryption in transit but does not include encryption at rest. Encrypting data at rest is an important cybersecurity objective for connected vehicles and should be included in the chart.	The Coalition suggests that NIST add encryption at rest as an objective for connected vehicle cybersecurity.
5	The Coalition for Cybersecurity Policy & Law	Major	Line 1577 Page 42	Table 3 is a helpful depiction of the cybersecurity risks facing health IoT and medical devices. The Coalition believes that creating a similar table for each of the IoT applications addressed in the Report will provide a useful resource for readers to understand these risks.	The Coalition encourages NIST to adapt Table 3, which appears in the discussion of the risks for health IoT and medical devices, to create similar tables that identify the risks for each of the IoT applications discussed in the Report.
6	The Coalition for Cybersecurity Policy & Law	Minor	Lines 1676 – 1717 Page 46	The list of important security considerations for securing IoT applications is very helpful for readers to understand the considerations at issue when reading the rest of the Report. The Coalition believes that this list would be more helpful to readers if it appeared earlier in the Report.	The Coalition encourages NIST to move the list of important considerations for securing IoT applications appearing at the beginning of section 8 to section 4.