February 11, 2020

Via iotsecurity@nist.gov

Katerina Megas
Program Manager
Cybersecurity for the Internet of Things (IoT) Program
National Institute of Standards and Technology
Gaithersburg, MD 20899

Michael Fagan
Computer Scientist
Cybersecurity for the Internet of Things (IoT) Program
National Institute of Standards and Technology
Gaithersburg, MD 20899

Subject: Draft (2nd) NISTIR 8259, *Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline*

Dear Ms. Megas, Mr. Fagan, and Colleagues:

The U.S. Chamber of Commerce commends your efforts in developing the draft (2nd) NISTIR 8259, *Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline* (NISTIR 8259). We appreciate the National Institute of Standards and Technology's (NIST's) engagement with the Chamber and other business organizations. NISTIR 8259 reflects the close rapport that has been cultivated between NIST and industry leaders over the past several years to strengthen U.S. cybersecurity, including critical infrastructure and the Internet of Things (IoT).[1]

SUMMARY

- The Chamber strongly supports the efforts of National Institute of Standards and Technology (NIST) officials to develop a core Internet of Things (IoT) cybersecurity baseline in partnership with industry.

- Revised language in the draft (2nd) NISTIR 8259, *Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline* (NISTIR 8259), provides constructive, voluntary recommendations for device manufacturers to consider before and after IoT devices are produced. However, the Chamber preferred the relative prominence of the core baseline in the first draft of NISTIR 8259 (i.e., section 4 and table 1).[2]

- The Chamber believes that NIST and industry have a shared interest in publishing the core baseline as a stand-alone document for the core baseline to have maximum effect on IoT device cybersecurity and resilience.

- The Chamber urges NIST to reinforce to stakeholders, especially policymakers, that the purpose of NISTIR 8259 and the core baseline is to give manufacturers nonregulatory recommendations for improving the security of new IoT devices.

Separating the Core Baseline and Foundational Activities Into Two Documents

NIST made some notable enhancements to the sections of NISTIR 8259[3] that accompany The Core Device Cybersecurity Capability Baseline for Securable IoT Devices (table 1). However, the Chamber's main urging from this past fall—that the core baseline and the adjacent guidance in NISTIR 8259 should be separated—remains unaddressed.[4] In the Chamber's view, NISTIR 8259 should explicitly distinguish between the document's comparatively expansive *foundational activities* and the *core baseline*, which has a tighter focus. The blending of these two elements of NISTIR 8259 could unintentionally lessen the value of the core baseline in commercial and policy settings in ways that neither NIST nor industry wants to promote.

The latest version of NISTIR 8259 appears to subsume the core baseline within one of six foundational activities (Activity 3: Determine How to Address Consumer Goals), which clouds the distinction between the foundational activities and the core baseline that many in industry seek to elevate. The Chamber urges NIST to make the separation between the foundational activities and the core baseline obvious to readers of NISTIR 8259.

The core baseline is deeply grounded in public-private consensus and potentially not in harmony with many of the adjoining foundational activities. The latter content relies on the ongoing work of multiple IoT device security guidance documents published by private standard-development groups and government agencies. The foundational activities do not yet represent industry-government consensus because they are still being shaped and debated by many cyber stakeholders.

The Chamber believes that while well intentioned, the placement of the core baseline within a foundational activity will weaken the importance of the core baseline in the marketplace and give outsize weight to noncore activities, such as communicating to customers (Activities 5 and 6). For example, although the considerations in Activities 5 and 6 are written as a series of optional questions that manufacturers can answer, their inclusion as foundational parts of the document may be misinterpreted by courts, regulators, and policymakers as security requirements. The lack of a clear wall separating foundational activities from the core baseline will have practical outcomes.

If IoT device manufacturers say that they use NISTIR 8259, it will be unclear to them and others what *use* means. Will use mean conforming to the core baseline? Or will it mean addressing all the questions that the foundational activities encourage manufacturers to take up? It is too soon to tell, but such confusion may decrease the likelihood that manufacturers will actively leverage NISTIR 8259. Further, the Chamber anticipates seeing references to NISTIR 8259 in federal and/or state laws and wants to minimize any unintended consequences. We foresee manufacturers, and even a fair number of commercial buyers, having concerns about legal liability because of the lack of

clarity regarding the core baseline and the foundational activities. A point of reference is the Ohio Data Protection Act (ODPA), which became law in 2018.

ODPA aims to enhance the cybersecurity of Ohio businesses. It provides an affirmative defense (also referred to in the act as a "safe harbor") against tort claims arising from a data breach to businesses showing that they have implemented one of several industry recognized frameworks and/or federal laws or regulations that a business may reasonably conform to.[5] ODPA lists the joint industry-NIST *Cybersecurity Framework* (the *Framework*) as an approved "cybersecurity framework." The key point is that the law references the entire *Framework*, not just a particular section or table inside it. There is robust support for the full *Framework* in the public and private sectors.

The Chamber would likely support a federal or state law that creates an affirmative defense for users of the core baseline, but not the entire NISTIR 8259, owing largely to the fact that there is not yet strong industry recognition for many aspects of NISTIR's noncore foundational activities.

Emphasizing the Nonregulatory Intent of NISTIR 8259 and the Core Baseline

NIST and the business community should prepare for regulatory entities, legislatures, and judicial bodies to misread NISTIR 8259 as prescriptive. Despite NIST's stressing that the guidance to manufactures on IoT device security is thoroughly voluntary—the Chamber counted at least five mentions in the document—NISTIR 8259 will need to send a clear signal to government officials that neither the foundational activities nor the core baseline should be construed as regulatory in nature.

On a more granular level, the Chamber urges NIST to change the middle column header of the core baseline to "Potential Elements" or "Example Elements" from "Key Elements." On page 11, NISTIR 8259 says, "The second column provides a numbered list of *key elements* of that capability—elements an IoT device manufacturer seeking to implement the core baseline often (but not always) would use in order to achieve the capability. (Note: the elements are not intended to be comprehensive, nor are they in any particular order)" [italics in the original]. The term Key Elements could lead some readers to interpret them as requirements, not as voluntary recommendations, which is NIST's objective. Hence, NISTIR 8259 should be changed to reflect this thinking.

Table 1: The Core Device Cybersecurity Capability Baseline for Securable IoT Devices

Device Cybersecurity Capability	~~Key Elements~~ Potential Elements or Example Elements	IoT Reference Examples

***

NIST is a valued partner of the Chamber on an array of business issues, especially cybersecurity. We believe that NIST appreciates our concerns regarding the direction of NISTIR 8259. The Chamber is not asking NIST to abandon the foundational activities listed in NISTIR 8259, which agency officials have worked diligently to develop. We believe, though, that NIST and industry have a mutual interest in publishing the core baseline as a self-contained document for it to have maximum effect regarding IoT security and resilience.

If you have any questions or need more information, please do not hesitate to contact Christopher Roberti (croberti@uschamber.com, 202-463-3100) or Matthew Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,

Christopher D. Roberti
Chief of Staff
Senior Vice President, Cyber, Intelligence, and Security

Matthew J. Eggers
Vice President, Cybersecurity Policy

Notes

[1] www.uschamber.com/sites/default/files/10-24-18_u.s._chamber_comment_letter_draft_nistir_8228_final.pdf
www.uschamber.com/sites/default/files/2-7-19_multi-association_wh_letter_iot_cybersecurity_final.pdf

[2] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf

[3] https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259-draft2.pdf

[4] www.uschamber.com/sites/default/files/09-30-19_uscc_comment_letter_nistir_8259_final_v1.0.pdf

[5] Also, the Ohio law does not set minimum cybersecurity requirements for data protection or privacy or establish a basis for a private right of action.
www.legislature.ohio.gov/download?key=10218&format=pdf
https://moritzlaw.osu.edu/data-and-governance/wp-content/uploads/sites/105/2019/03/cybersecurity-whitepaper-32819F-1.pdf
https://cyber.ohio.gov/wps/portal/gov/cyber/presentations/resources/senate-bill-220-the-data-protection-act