U.S. CHAMBER OF COMMERCE

September 30, 2019

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 NISTIR 8259, *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers*

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

The U.S. Chamber of Commerce generally supports the draft NISTIR 8259, *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers* (NISTIR 8259).[1] We appreciate the substantial effort that you and your colleagues put into developing it, especially engaging the Chamber and other business groups. 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 small and midsize businesses, critical infrastructure, and the Internet of Things (IoT).[2]

Summary

- The core IoT security baseline (section 4/table 1) in draft NISTIR 8259 is a quality starting point for device security. However, the baseline and the adjacent guidance (sections 3, 5, 6, and 7) in the NISTIR should be separated, with the latter being placed in an accompanying roadmap. The NISTIR 8259 baseline and the *C2 Consensus on IoT Security Baseline Capabilities* (C2 Consensus) are complementary and flexible efforts.

- IoT cyber stakeholders should increasingly direct their activities toward fostering market demand for strong devices and pressing public officials at home and internationally to align their policies to the industry-driven baseline.

- Policymakers need to match industry's leadership concerning IoT standards development, device security, and resilience. IoT cyber legislation needs to be passed that reflects the baseline, protects device makers and buyers, reduces policy fragmentation globally, and bolsters collective defense.

SUBSTANTIAL PROGRESS TOWARD STRENGTHENING IOT SECURITY

In addition to backing NISTIR 8259, the Chamber is bullish on the C2 Consensus. The Chamber participated in the creation of the C2 consensus baseline, led by the Council to Secure the Digital Ecosystem (CSDE).[3] The C2 Consensus provides experienced guidance to the public and private sectors on securing new IoT devices to (1) raise the market's expectations for security and (2) advance policy harmonization globally. C2 Consensus parties expect that this orientation toward international harmonization will enhance security more effectively compared with a number of troubling regional or local initiatives that industry is witnessing domestically and overseas.

Fragmented approaches to IoT cyber will lead to duplicative and/or confusing security requirements, splinter organizations' risk management budgets, and cause market distortions that will weaken security for individual companies and collectively.

ONGOING GOALS: FOSTERING DEMAND FOR STRONG DEVICES AND ALIGNING POLICY TO THE INDUSTRY-LED BASELINE

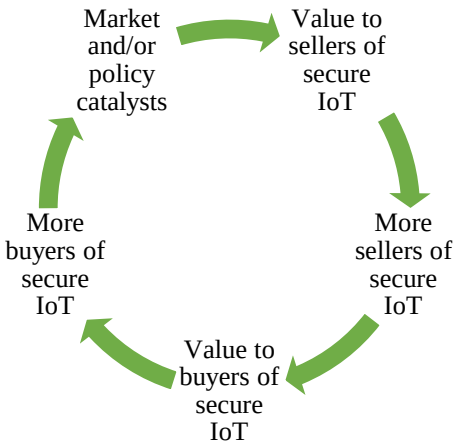
NISTIR 8259 and the C2 Consensus are complementary and flexible documents;[4] their baselines overlap to a remarkable extent. In the short run, voluntary and internationally accepted IoT security standards will need to be written by industry and government experts to express the guidance of both NISTIR 8259 and the C2 Consensus in a technically precise manner suitable for device manufacturers and related stakeholders.

Meanwhile, the Chamber believes that stakeholders should increasingly direct their energies toward accomplishing two goals that will bolster the promotion of the baseline: (1) fostering market demand for strong devices and (2) pushing public officials at home and internationally to align their policies to the industry-driven IoT cyber baseline.

Securable Devices Need to Be Built and Bought

First, the impressive work undertaken by NIST and the C2 Consensus may not be fully realized without a clear and growing demand for securable devices. Market demand is growing, but it needs to be cultivated.[5] It won't be enough for securable IoT technologies to be designed and built; they need to be bought. To achieve this objective, the Chamber envisions a broad array of stakeholders promoting the production, purchase, and deployment of more secure IoT products across the U.S. and globally.

Put simply, the Chamber wants device makers, service providers, and buyers to profit from the business community leading the development of state-of-the-art IoT components and sound risk management practices. This allied group will likely be composed of parties whose interests vary but are united toward a common objective—improving the security and resilience of the emerging IoT ecosystem.[6]



Which comes first—strong devices or strong market demand? Stakeholders are trying to think through and solve a chicken and egg strategy problem.[7]

U.S. and International Policies Need to Be Aligned to the Baseline

The Chamber wants to spur commercial demand for strong devices by consumers (e.g., public and private enterprises and households). The second involves pushing policymakers at home and abroad to align their policies to the industry-led baseline. There is a robust consensus that IoT cyber efforts will be most effective if they reflect global standards and innovative commercial practices, especially NISTIR 8259 and the C2 Consensus. Industry advocacy will take at least three forms:

- **Supporting U.S. leadership in international IoT cyber forums.** Standards, guidance, and best practices relevant to cybersecurity are typically led by the private sector and adopted on a voluntary basis; they are optimal when developed and recognized globally. Such approaches avoid burdening IoT cyber stakeholders with requirements coming from multiple, and often conflicting, jurisdictions. The Chamber appreciates that NIST has been actively meeting with foreign parties (e.g., the European Union) to press them to embrace an IoT security capabilities baseline. The Chamber urges the administration to work with international partners and believes that these discussions should be multistakeholder driven and occur routinely.[8]

- **Spotlighting global alignment to an industry-led baseline.** The Chamber believes that policymakers in the U.S. and internationally need to align their IoT security and resilience programs with the baseline reflected in NISTIR 8259 and the C2 Consensus. Achieving general agreement between the business community and policymakers will streamline and strengthen government-industry collaboration on IoT security and enable the U.S. to champion an IoT security baseline worldwide. This method will ensure stakeholders' cybersecurity concerns are adequately addressed and that IoT security requirements do not become a barrier to trade.

- **Reducing regulatory fragmentation.** There is a market need for a common IoT cyber security baseline—owing to a growing number of often disparate policy proposals and requirements—to chart a path for businesses and standards bodies to follow. A fragmented global cybersecurity environment creates much uncertainty for device makers and buyers and splinters the resources that businesses devote to sound device development, production, and assessments.

FEEDBACK ON NISTIR 8259: NON-BASELINE GUIDANCE SHOULD BE PLACED IN AN ACCOMPANYING ROADMAP

On a more granular level, feedback that the Chamber has received from our members regarding NISTIR 8259 roughly falls into two categories. First, NIST should distinguish between finished devices and device components in terms of what the baseline applies to. The features for securable IoT devices are configured at the device level and are a function of embedded systems and engineering. They should be viewed holistically. An IoT device is a finished product available to consumers, which is used for its intended purposes without being embedded or integrated into another product and is not a component.

Second, NISTIR 8259 improves upon NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, which was first published in the fall 2018. The Chamber thinks that the additional non-baseline guidance included in NISTIR 8259—feature implementation (section 3), feature implementation (section 5), customer information (section 6), and secure development practices (section 7)—is valuable to discuss as part of IoT device security. Some industry organizations believe that sections 3, 5, 6, and 7 are worthy of being included in the final NISTIR 8259.

However, a number of business groups argue that there should be a clear delineation between the baseline and the adjoining guidance. According to this viewpoint, NISTIR 8259 section 4/table 1 constitutes a baseline for new devices. But supplemental sections 3, 5, 6, and 7 do not fit the concept of a baseline, which could be misleading to businesses and policymakers. Further, the structure of NISTIR 8259 should reflect two ideas. First, the baseline for IoT cybersecurity is the dominant element of NIST's guidance. Second, the guidance for manufacturers, while constructive, is not yet core to device security and should be separated from section 4/table 1 to avoid stakeholder confusion.[9]

Thus, the Chamber urges NIST to include sections 3, 5, 6, and 7 in an adjoining roadmap. A roadmap was successfully utilized in the context of the *Cybersecurity Framework* to handle areas that were not ready for inclusion in the framework and/or required ongoing development and consensus building.[10] Such an approach would respect multiple viewpoints, allow work to continue on the non-baseline sections, and enable the baseline to move forward.

THE BASELINE AND FEDERAL LEGISLATION

In June 2019, the Senate Homeland Security and Governmental Affairs Committee and the House Oversight and Reform Committee passed their respective versions of the IoT Cybersecurity Improvement Act of 2019 (S. 734 and H.R. 1668). The committees reported amendments in the nature of a substitute (ANS or substitute amendments) to the underlying legislation. The substitute amendments are different both from one another and the original legislation that was introduced last spring. The Chamber commends the bill writers for capturing in the legislation that industry and NIST are developing a baseline for IoT devices. This recognition is a key change from the last Congress.

Further Discussions Required: IoT Cyber Legislation, Collective Defense

The Chamber urges additional dialogue with lawmakers and staff on whether to define IoT in legislation and the specifics of the coordinated vulnerability disclosure (CVD) program.[11] Meanwhile, it needs to be stressed that lawmakers' work remains incomplete. First, Congress should consider a national, more sustainable way to bolster IoT cybersecurity, rather than regulating the federal market for IoT devices. Such an approach is critical to reducing the expanding policy and regulatory fragmentation that is taking place domestically and overseas.[12]

The Chamber urges Congress to develop legislation that would both spur device makers to build to the cyber baseline and grant legal liability and regulatory protections to the makers and sellers of strong IoT equipment. Legislation of this kind would be a win-win for government and industry.

Second, S. 734 and H.R. 1688 presuppose devices being hacked illegally, but they do not put pressure on malicious actors that threaten connected devices and their underlying networks. Policymakers should not place new mandates on businesses while leaving cyberattackers untouched. The Chamber made this argument to bill writers in 2017, and yet it has gone unaddressed. The legislation needs to elevate the government's portion of the security burden to make the mantra that cybersecurity is a shared public-private responsibility more meaningful. As currently written, S. 734 and H.R. 1688 put the defense of IoT devices, particularly against nation-states hackers or their surrogates, on the shoulders of the private sector. Businesses should not have to contend with top cyber threats (e.g., Russia, China, Iran, and North Korea) seemingly single-handedly.[13]

The Chamber welcomes the opportunity to provide feedback on NISTIR 8259. We are optimistic about the future of the IoT, which continues the decades-long trend of connecting networks of objects through the internet. The IoT will significantly affect many aspects of the economy, and the Chamber wants to constructively shape the breadth and nature of its eventual impact. Many observers predict that the expansion of the IoT will bring positive benefits through enhanced integration, efficiency, and productivity across many sectors of the U.S. and global economies.

Significant aspects of the IoT, including guarding against botnets and other automated threats, will also influence economic growth, infrastructure, cities, and individual consumers.[14] NISTIR 8259 tracks closely with fundamental cybersecurity principles that the Chamber extensively advocates for to foster beneficial outcomes of the IoT.[15] 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

Endnotes

[1] See https://csrc.nist.gov/publications/detail/nistir/8259/draft. Draft NISTIR 8259, released in July 2019, builds upon NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, which was initially published in September 2018.

[2] In February 2019, 24 associations sent a letter to the White House urging the administration and Congress to support NIST's efforts alongside industry to bolster IoT security.
www.uschamber.com/sites/default/files/2-7-19_multi-association_wh_letter_iot_cybersecurity_final.pdf

[3] See https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf. The U.S. Chamber of Commerce is one of some 20 organizations that endorsed the September 2019 *C2 Consensus on IoT Security Baseline Capabilities*.

[4] NISTIR 8259 "presents a core baseline of cybersecurity features for all IoT devices that makes devices at least minimally securable by the customers who acquire and use them. This publication does not specify how customers should secure the IoT devices they deploy and use. . . ." Further, the baseline's features are "not intended to be fully adopted by every IoT device; every IoT device has a unique set of expected customers and use cases, and not all features in the core baseline will make sense to use in every situation"
(pages viii, 16).

[5] The November 2019 *Botnet Road Map* calls for establishing robust markets for consumer and industrial devices.
www.ntia.doc.gov/blog/2018/road-map-building-more-resilient-internet

[6] The Chamber is assessing the establishment of a Buy Strong IoT Coalition to promote the production, purchase, and deployment of more secure IoT products. If created, the coalition would explore facilitating a process in the marketplace that generates both security and value for buyers and sellers. Market and/or policy incentives may be needed to initiate progress, but the specifics are yet to be determined.

[7] This graphic was inspired, in part, by the Strategic Toolkits webpage, "Chicken and Egg Strategy Problems."
http://strategictoolkits.com/strategic-concepts/chicken-and-egg-strategy-problems

[8] Moreover, the U.S. benefits when industry and the federal government effectively influence the development or revision of international technology standards. The smart development of international standards concerning IoT and 5G deployments, for example, advances U.S. commercial and security priorities by facilitating constructive outcomes—including improved interoperability, greater trust in online transactions, and strengthened competitiveness of American products and services.

There is a strong relationship between standards and innovation that U.S. officials and the Chamber have a shared interest in promoting. Assertive and sustained U.S. engagement in standards bodies is instrumental to America's economic well-being. The standards development process should continue to be industry led, open, consensus based, and balanced. Specifically, there should be meaningful involvement from a broad range of parties—including any business that is interested in participating—to prevent any single group, foreign nation, or company from dominating the decision making.
www.uschamber.com/sites/default/files/190816_comments_tglextension_bis_final_v1.0.pdf

[9] The Chamber agrees with draft joint comments written by the Consumer Technology Association and USTelecom. They argue that sections 3, 5, 6, and 7 could be viewed unintentionally as "hard requirements in procurement, retail, and regulatory setting."

[10] www.nist.gov/cyberframework/related-efforts-roadmap

[11] www.uschamber.com/sites/default/files/07-2-19_uscc_prelim_feedback_iot_cyber_leg_s734_and_hr1668_substitute_amdts_final_v1.0.pdf

[12] The Chamber testified before a Senate Commerce, Science, and Transportation Committee subcommittee in April 2019, saying that a fragmented cybersecurity environment—including S. 734 and H.R. 1668, California's device security law, and the European Union's Cybersecurity Act—creates uncertainty for device makers and buyers and splinters the resources that businesses devote to sound device development, production, and assessments.
www.commerce.senate.gov/public/index.cfm/2019/4/strengthening-the-cybersecurity-of-the-internet-of-things

[13] www.acq.osd.mil/dsb/reports/2010s/dsb-cyberdeterrencereport_02-28-17_final.pdf

[14] See, in particular, comments submitted to NTIA by C_TEC in March 2017 and June 2016.
www.ntia.doc.gov/files/ntia/publications/comments_of_c_tec_3-13-17.pdf
www.ntia.doc.gov/files/ntia/publications/cati.iotcommentsfinal.pdf

[15] In July 2017, the Chamber submitted comments to NTIA's notice *Promoting Stakeholder Action Against Botnets and Other Automated Threats*.
www.ntia.doc.gov/files/ntia/publications/us_chamber_letter_botnets_iot_cybersecurity_final.pdf

See related Chamber comments submitted to NTIA concerning botnets and IoT in February 2018.
www.ntia.doc.gov/files/ntia/publications/us_chamber_of_commerce.pdf

See, too, *The IoT Revolution and Our Digital Security: Principles for IoT Security*, September 2017, written by the Chamber and Wiley Rein LLP.
www.uschamber.com/IoT-security

NIST *IoT Cybersecurity Colloquium*, October 2017.
www.nist.gov/news-events/events/2017/10/iot-cybersecurity-colloquium
www.nist.gov/sites/default/files/documents/2017/10/23/matttheweggers_slides.pdf