U.S. CHAMBER OF COMMERCE

October 24, 2018

Via iotsecurity@nist.gov

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

Subject: Draft NIST Interagency Report (NISTIR) 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*

Dear Ms. Megas and Colleagues:

The U.S. Chamber of Commerce generally supports the draft NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* (NISTIR). We appreciate the substantial effort that you and your colleagues put into developing it, including meeting with the business community in multiple forums.

First, we agree with the National Institute of Standards and Technology's (NIST's) decision to leave IoT undefined.[1] Each sector has its own types of IoT devices (e.g., specialized medical equipment in the health care sector and smart automobile technologies in the transportation sector). Connected consumer devices are quickly proliferating (e.g., refrigerators, thermostats, and TVs).[2]

What's especially important, the NISTIR says that organizations should mitigate risks to connected devices' cybersecurity and privacy throughout their life cycles—but it empowers organizations to determine which considerations and challenges apply to particular IoT equipment.

Second, the NISTIR captures stakeholders' interest in continued engagement on so-called cybersecurity and privacy baselines for IoT devices.[3] NIST is not reinventing the wheel, which is key for policymakers to understand. The agency is, in part, leveraging extensive public and private sector initiatives that are underway to enhance the security and privacy of IoT devices.[4]

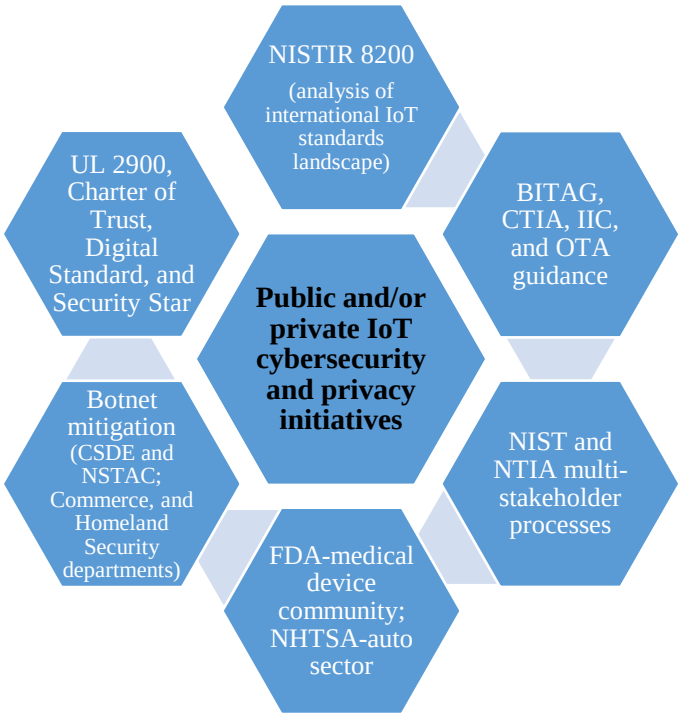
SUMMARY

- The Chamber generally supports the NISTIR, which stresses that organizations should mitigate cybersecurity and privacy risks to IoT devices. However, the report enables organizations to determine which considerations apply to certain connected devices.
- The Chamber urges the Department of Commerce to convene additional discussions with industry and other cyber stakeholders on nonregulatory baselines for IoT devices.

We strongly agree with NIST's view that stakeholders should establish IoT device security and privacy capabilities with humility.

- The Chamber wants device makers, service providers, and buyers to gain from the business community leading the development of state-of-the-art IoT components and risk management practices. Next steps include catalyzing a process in the market that generates increased security and value for buyers and sellers.

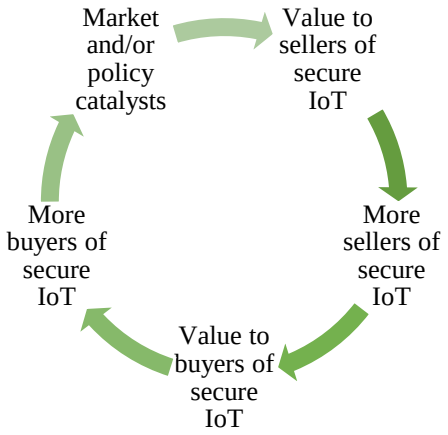
Public and/or private IoT cybersecurity and privacy initiatives (select examples)[5]



The Chamber urges the Department of Commerce to convene additional discussions with industry and other cyber stakeholders on baselines. The Chamber believes that industry should drive the security and resilience of the IoT ecosystem in collaboration with public entities, which need to prioritize pushing back on malicious actors. NIST says that it intends to develop a future publication "defining a high-level baseline and one or more publications defining baselines and other recommendations for particular IoT device types." The Chamber wants to engage such undertakings.

The Chamber contends that NIST and industry need to collaborate to debate and possibly determine baseline security and privacy recommendations that are recognized globally, rather than defer decision making to regional bodies (e.g., the EU),[6] Congress, or state legislatures.[7] At the same time, the Chamber strongly agrees with NIST's view that stakeholders should set IoT device security and privacy baselines with humility.[8] Indeed, NIST notes that because IoT devices and their uses and needs are so varied, "few recommendations can be made that apply to all IoT devices."[9]

Third, the Chamber wants device makers, service providers, and buyers to gain from the business community leading the development of state-of-the-art IoT components and sound risk management practices. Stakeholders are trying to solve a chicken-and-egg strategy problem. Next steps include 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 jumpstart this circle.[10]



The Chamber welcomes the opportunity to provide feedback on the NISTIR. 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.

Meaningful aspects of the IoT, including guarding against botnets and other automated threats, will also influence economic growth, infrastructure and cities, and individual consumers.[11] The NISTIR tracks closely with fundamental cybersecurity principles that the Chamber extensively advocates for to foster beneficial outcomes of the IoT.[12]

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] The National Telecommunications and Information Administration's (NTIA's) January 2017 *Green Paper: Fostering the Advancement of the Internet of Things* is a significant policy paper regarding the development of the IoT. Some parties argue that strict definitions or labels could inadvertently narrow the scope of the IoT's potential applications (pg. 5). www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[2] Draft NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* (NISTIR), September 24, 2018, pg. v. https://csrc.nist.gov/news/2018/nist-releases-draft-nistir-8228-for-comment https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf

[3] The NISTIR says, "The term 'baseline' has different meanings to different people and organizations. Some want flexible general recommendations; some want specific, prescriptive guidance; and the rest want something in between. In this publication, 'baseline' is used in the generic sense of a set of requirements or recommendations. It should not be confused with the low, moderate, and high control security baselines set forth in NIST Special Publication 800-53 to help federal agencies meet their obligations under the Federal Information Security Modernization Act (FISMA) and other federal policies" (pg. iv).

[4] NISTIR, pg. 29.

[5] Starting with the draft NISTIR 8200 and moving clockwise, see the following examples, which the Chamber does not necessarily endorse:

- Draft NISTIR 8200, *Status of International Cybersecurity Standardization for Internet of Things (IoT)*. www.nist.gov/sites/default/files/documents/2018/04/19/4-18-18_uscc_letter_nist_draft_nistir_8200_final.pdf
- The NISTIR references guidance from the Broadband Internet Technical Advisory Group (BITAG), etc. (pg. 30).
- NIST and NTIA multistakeholder processes. www.ntia.doc.gov/IoTSecurity and www.ntia.doc.gov/category/internet-things
- "Statement from FDA Commissioner Scott Gottlieb, M.D. on FDA's efforts to strengthen the agency's medical device cybersecurity program as part of its mission to protect patients," FDA, October 1, 2018. www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm622074.htm www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf
- National Highway Traffic Safety Administration (NHTSA). www.nhtsa.gov/crash-avoidance/automotive-cybersecurity
- National Security Institute (NSI) policy paper, *Cyber Imperative: Preserve and Strengthen Public-Private Partnerships*, October 2018. See pg. 14 on public-private partnerships regarding IoT cybersecurity. https://nationalsecurity.gmu.edu/2018/10/nsi-policy-paper-cyber-imperative-preserve-and-strengthen-public-private-partnerships
- Council to Secure the Digital Economy (CSDE). www.ustelecom.org/news/press-release/ustelecom-and-iti-launch-council-secure-digital-economy
- National Security Telecommunications Advisory Committee (NSTAC) *Report to the President on Internet and Communications Resilience*, November 2017. www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf www.ntia.doc.gov/press-release/2018/us-departments-commerce-homeland-security-release-report-president-promoting

- UL 2900. https://industries.ul.com/cybersecurity/ul-2900-standards-process
- Charter of Trust. www.siemens.com/press/pool/de/feature/2018/corporate/2018-02-cybersecurity/charter-of-trust-e.pdf
- The Digital Standard. www.thedigitalstandard.org
- Security Star. www.publicknowledge.org/assets/uploads/documents/Securing_the_Modern_Economy--Transforming_Cybersecurity_Through_Sustainability_FINAL_4.18.18_PK.pdf

[6] EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act). 2017/0225(COD), September 2017.
www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2017/0225(COD)

In August 2017, the Chamber and six European organizations sent a letter to the European Commission regarding "measures on cybersecurity standards, certification and labelling to make ICT-based systems, including connected objects." The industry groups argued that Europe, like the U.S., can expect to benefit from economic growth brought about by the expanding IoT as long as policymakers cultivate a digital environment that avoids misguided regulations and supports pioneering businesses. Underpinning the Chamber's efforts at home and abroad is advocacy for smart policies for smart devices. www.uschamber.com/iot%26cybersecurity

[7] On January 1, 2020, California SB-327 will require a manufacturer of a connected device to equip the device with a "reasonable security feature or features" that are appropriate to the nature and function of the device, among other requirements. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

[8] House Oversight and Government Reform Committee's Information Technology Subcommittee hearing, *Cybersecurity of the Internet of Things*, October 3, 2017.
https://oversight.house.gov/hearing/cybersecurity-internet-things
https://oversight.house.gov/wp-content/uploads/2017/10/Eggers_Testimony_IOT_10032017.pdf

[9] NISTIR, pg. iv.

[10] 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

[11] See, in particular, comments filed with the NTIA by the 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

[12] In July 2017, the Chamber submitted comments to the 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 on February 12, 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 18, 2017.
www.nist.gov/news-events/events/2017/10/iot-cybersecurity-colloquium
www.nist.gov/sites/default/files/documents/2017/10/23/matthewweggers_slides.pdf