Statement of the U.S. Chamber of Commerce

ON: ***Strengthening the Cybersecurity of the Internet of Things***

TO: Senate Commerce, Science, and Transportation Committee Security Subcommittee

DATE: April 30, 2019

1615 H Street NW | Washington, DC | 20062

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations. The Chamber is dedicated to promoting, protecting, and defending America's free enterprise system.

More than 96% of Chamber member companies have fewer than 100 employees, and many of the nation's largest companies are active members. We are therefore cognizant not only of the challenges facing smaller businesses but also those facing the business community at large.

Besides representing a cross-section of the American business community with respect to the number of employees, major classifications of American business—for example, manufacturing, retailing, services, construction, wholesalers, and finance—are represented. The Chamber has membership in all 50 states.

The Chamber's international reach is substantial as well. We believe that global interdependence provides opportunities, not threats. In addition to the American Chambers of Commerce abroad, an increasing number of our members engage in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Matthew J. Eggers
Vice President, Cybersecurity Policy, U.S. Chamber of Commerce
Senate Commerce, Science, and Transportation Committee
Security Subcommittee
Strengthening the Cybersecurity of the Internet of Things
April 30, 2019

SUMMARY

- **Industry and National Institute of Standards and Technology (NIST) leadership.** The business community, NIST, and other stakeholders are developing a core cybersecurity capabilities baseline for Internet of Things (IoT) devices. A top U.S. Chamber of Commerce priority for industry is to achieve consensus on the technical criteria that support the IoT cyber baseline.

- **A win-win cybersecurity market.** The Chamber wants device makers, service providers, and buyers to gain from the development of state-of-the-art IoT components and sound risk management practices.

- **Global, industry-driven standards and practices.** The Chamber believes that IoT cyber efforts will be most effective if they reflect global standards and industry-driven practices. A fragmented global cybersecurity environment creates uncertainty for industry and splinters the resources that businesses devote to device development, production, and assessments.

Good afternoon, Chairman Sullivan, Ranking Member Markey, and other distinguished members of the Security Subcommittee (subcommittee). My name is Matthew Eggers, and I am the vice president of cybersecurity policy with the U.S. Chamber of Commerce's Cyber, Intelligence, and Security Division (CISD). On behalf of the Chamber, I welcome the opportunity to testify before the subcommittee regarding enhancing the cybersecurity and resilience of the Internet of Things (IoT). The Chamber welcomes the subcommittee's dedication to examining pressing cyber matters.

The Chamber's CISD was established in 2003 to develop and implement the Chamber's homeland and national security policies. The division's Cybersecurity Working Group (CWG), which I lead, identifies current and emerging issues, crafts policies and positions, and provides analysis and direct advocacy to government and business leaders.

In addition to the CWG, I want to highlight two other groups within the Chamber that address IoT—the Chamber Technology Engagement Center (C_TEC) and Project Security, which handles our international cyber initiatives. C_TEC is at the forefront of advancing IoT deployment and innovation in the digital economy. Its initiatives include working groups on autonomous vehicles, 5G, and unmanned aerial vehicles.[1]

Project Security is a partnership between CISD and the Center for Global Regulatory Cooperation (GRC), which is housed in the Chamber's International Division. Project Security works with foreign governments and multilateral forums to promote international alignment to flexible, globally accepted risk-based approaches to cybersecurity.

Project Security has engaged more than 30 foreign governments as they create and implement their respective cybersecurity programs. This engagement includes the European Commission (EC) and European Union (EU) national authorities regarding the Cybersecurity Act. The act establishes EU-wide cyber certification schemes for information and communications technology (ICT) products, services, and processes, including IoT devices.[2] Project Security leaders meet regularly with EU officials to negotiate constructive outcomes on IoT cybersecurity. It is also works with other international stakeholders, such as Japan, Singapore, Australia, and the U.K., to fashion consensus and industry-driven policy approaches to IoT security.[3]

I recognize that the subcommittee is considering legislation that addresses IoT cybersecurity. However, I will confine my written statement to (1) highlighting some key problems that face the IoT cyber market, (2) discussing industry and NIST collaboration toward a core IoT cybersecurity baseline, and (3) soliciting the subcommittee's assistance and counsel in elevating the fruits of this partnership at home and overseas.

Framing Key IoT Cybersecurity Challenges

It is important to frame some of the central challenges that impact the IoT cyber marketplace before discussing solutions.[4] In speaking at length with stakeholders over the last two years, the Chamber has identified several challenges associated with IoT cybersecurity:

- **Security risk.** IoT objects are potentially vulnerable targets for hackers. As the number of IoT devices grows, so will the potential risk of successful intrusions and increases in costs from those incidents.[5] Strong IoT security should be a win-win proposition for the makers and purchasers of robust devices, as well as U.S. economic and national security.[6]

- **Technical standards.** Industry and government share an interest in fostering stronger IoT security and resilience. The business community and NIST are working diligently to deliver a core capabilities baseline for IoT devices that increases security, is dynamic in the face of threats, and is scalable internationally. A top Chamber priority will be for industry to achieve consensus on the technical criteria that support the IoT cyber baseline, including for consumer and industrial devices.

- **Public policy mandates.** The Chamber is concerned about policies at home and abroad that require specific, top-down approaches to security. Such mandates are unlikely to keep up with malicious actors or align with international best practices—outcomes that the Chamber presses the public and private sectors to pursue.[7]

- **Buyer decision making.** A number of IoT cyber advocates take a "build it and they will come" approach to IoT cyber, which tracks with traditional, rational notions of economics. Yet it is unclear if buyers—including individuals, households, businesses, and public institutions—will (1) pay for the cost of additional security features or (2) be able to identify a strong device without a nonregulatory tool to help them make educated choices.[8]

  Most people's intuition is to buy the least expensive device even if the device's security is not strong—and possibly contrary to their own best interests. The Chamber seeks to better understand how people make real-world choices regarding purchasing IoT technology.[9] The Chamber wants to get strong devices into the networks of businesses and the hands of consumers. Among other things, strong IoT will yield positive externalities.[10]

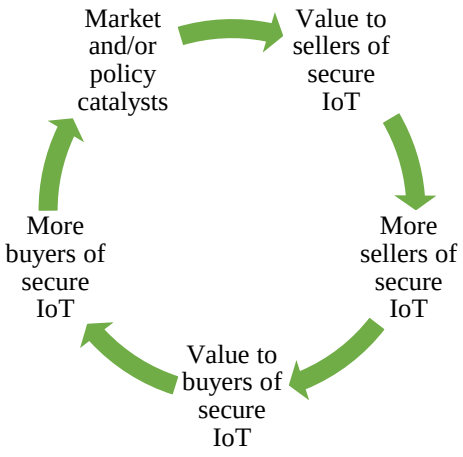
Industry and NIST Are Developing a Core IoT Cybersecurity Baseline

On February 7, 2019, the Chamber and 23 organizations sent a letter to the White House to urge the administration and Congress to support NIST's partnership with industry to strengthen IoT cybersecurity. The letter called on policymakers to support NIST in convening a robust effort on IoT security. Such an initiative will help stakeholders identify a flexible, performance-based, and cost-effective approach that can be voluntarily used by producers, sellers, and users of IoT devices to help them manage cyber risk and threats. The Chamber stressed three points in communicating with White House officials:

- **Complement existing work.** This initiative should advance NIST's ongoing IoT cyber work with industry, in keeping with NIST's February 2019 draft *Considerations for a Core IoT Cybersecurity Capabilities Baseline*; the September 2018 draft NIST Interagency Report (NISTIR) 8228, *Considerations for Managing IoT Cybersecurity and Privacy Risks*; and the administration's November 2018 *Botnet Road Map*.[11]

- **Elevate U.S. policy.** The undertaking should be elevated policywise to better compete with a number of IoT cyber proposals that are being developed at home and abroad. The Chamber wants this expedited effort to capture the imagination of public- and private-sector stakeholders—in essence, to serve as an IoT cyber rallying point—comparable to what the popular *Cybersecurity Framework* does for managing enterprise risks. Congress should boost the agency's funding, especially given the array of significant tasks that it undertakes with the private sector on cybersecurity and resilience.

- **Foster a market.** The *Botnet Road Map* calls for establishing robust markets for consumer and industrial devices. The Chamber wants device makers, service providers, and consumers to profit from the business community leading the development of state-of-the-art IoT components and practices. Stakeholders are trying to solve a chicken-and-egg strategy problem. Key next steps include advancing a market that generates both security and value for buyers and sellers. Market and/or policy incentives may be needed to jump-start this circle.[12]



IoT Cybersecurity Needs to Be Rooted in Global, Industry-Driven Standards and Practices

In 2015, the Chamber supported NISTIR 8074, *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, which served as a precursor to the November 2018 NISTIR 8200, *Status of International Cybersecurity Standardization for Internet of Things (IoT)*.[13] The Chamber contends that IoT cyber efforts will be most effective if they reflect global standards and industry-driven practices, including the joint industry-NIST core IoT security baseline. We urge Congress to leverage the following principles when crafting IoT security policy:

- **Support 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 multinational enterprises with the requirements of multiple, and often conflicting, jurisdictions.

  The Chamber appreciates that NIST has been actively meeting with foreign governments to urge them to embrace a core IoT security capabilities baseline. The Chamber urges the administration to work with international partners and believes that these discussions should be stakeholder driven and occur routinely.

- **Reduce regulatory fragmentation.** There is market demand for a common IoT cyber security baseline—due 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.

- **Spotlight global alignment with an industry-led baseline.** The Chamber believes that policymakers in the U.S. and abroad should align their IoT security and resilience programs with an industry-led IoT cyber capabilities baseline. Achieving consensus between the business community and NIST will streamline and strengthen government-industry collaboration on IoT security and enable the U.S. to champion more effectively a core IoT cyber baseline worldwide. This method should also ensure stakeholders' cybersecurity concerns are adequately addressed and that IoT security requirements do not become an unnecessary barrier to trade.

Thank you for giving me a chance to convey the Chamber's views. I am happy to answer any questions.

Endnotes

---

[1] The Chamber Technology Engagement Center (C_TEC).
https://www.uschamber.com/ctec

[2] In March 2019, the European Parliament approved a cybersecurity regulation commonly known as the Cybersecurity Act, which was initiated approximately two years ago.
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0151+0+DOC+PDF+V0//EN

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.
www.uschamber.com/sites/default/files/iot.cybersecurity.coalition._ec.letter.pdf

[3] See Chamber and Wiley Rein LLP paper *The IoT Revolution and Our Digital Security: Principles for IoT Security*, September 2017.
https://www.uschamber.com/IoT-security

[4] Readers of this testimony are encouraged to listen to "The Right Way to Solve Complex Business Problems," *Harvard Business Review*'s (HBR's) IdeaCast, December 4, 2018.
https://hbr.org/ideacast/2018/12/the-right-way-to-solve-complex-business-problems

[5] Eric A. Fischer, *The Internet of Things: Frequently Asked Questions*, Congressional Research Service (CRS), October 13, 2015, pg. 14.
https://fas.org/sgp/crs/misc/R44227.pdf

[6] Some 50 billion devices will be connected to the internet by 2020. According to the Chamber's estimates, the IoT could add roughly $15 trillion to global GDP over the next 20 years. See the Chamber's October 3, 2017, testimony before the House Oversight and Government Reform Committee Information Technology Subcommittee.
https://docs.house.gov/meetings/GO/GO25/20171003/106460/HHRG-115-GO25-Wstate-EggersM-20171003.pdf

[7] The Chamber would welcome clear steps by government officials to elevate their defense of industry and the IoT ecosystem.

[8] John Beshears and Francesco Gina, "Leaders as Decision Architects," HBR, May 2015. https://hbr.org/2015/05/leaders-as-decision-architects

[9] Richard H. Thaler, *Misbehaving: The Making of Behavioral Economics* (W.W. Norton and Company: New York, 2015).

[10] On positive externalities, see N. Gregory Mankiw, *Principles of Economics, Third Edition* (Thomson: U.S., 2004), pg. 207.

[11] NIST's Cybersecurity for the Internet of Things (IoT) Program. https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

The Council to Secure the Digital Economy (CSDE) and the Consumer Technology Association (CTA) are coordinating the development of an industry-led consensus—which its participants call the CSDE C2 (short for "convening the conveners")—regarding cybersecurity capabilities that will be common to new IoT devices. The CSDE C2 project will inform NIST's work, and vice versa, on identifying a core set of cybersecurity capabilities that could be a baseline for IoT devices.

Katerina Megas, "Let's talk about IoT device security," the National Institute of Standards and Technology (NIST), February 4, 2019.
https://www.nist.gov/blogs/i-think-therefore-iam/lets-talk-about-iot-device-security
https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf

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

Draft NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, September 24, 2018. The Chamber commented on NISTIR 8228 on October 24, 2018.
https://www.uschamber.com/sites/default/files/10-24-18_u.s._chamber_comment_letter_draft_nistir_8228_final.pdf

The Department of Commerce and the Department of Homeland Security (DHS), *Road Map: Building a More Resilient Internet* (aka the *Botnet Road Map*), November 29, 2018.
https://www.ntia.doc.gov/blog/2018/road-map-building-more-resilient-internet

[12] 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

[13] See April 18, 2018, Chamber letter to NIST on draft NISTIR 8200, *Status of International Cybersecurity Standardization for Internet of Things (IoT)*.
https://www.nist.gov/sites/default/files/documents/2018/04/19/4-18-18_uscc_letter_nist_draft_nistir_8200_final.pdf