IoT Cyber Policy

U.S. CHAMBER OF COMMERCE

IoT Cyber Policy

Matthew J. Eggers
Executive Director, Cybersecurity Policy
U.S. Chamber of Commerce

NIST *IoT Cybersecurity Colloquium*

October 19, 2017

Summary

- Economic growth
- Smart risk management principles
- Policies and objectives

Chamber policies and objectives (highlights)

1. Complex—no silver bullet to cybersecurity

2. Managing cyber risk across the ecosystem

3. Promote policies favorable to security and competitiveness

Chamber policies and objectives (cont.)

4. Embed in global and industry-driven standards

5. Public-private collaboration key

Federal IoT security policy initiatives (examples)

Bots

Medical devices

Patching and upgrading

Self-driving cars

“Smart cities” legislation

Warner/Gardner bill

Select resources

- *Transatlantic Cybersecurity* (Jan. 2017)—Chamber, Sidley

www.uschamber.com/TransatlanticCybersecurityReport

- *The IoT Revolution and Our Digital Security:*

Principles for IoT Security (Sept. 2017)—Chamber, Wiley Rein

www.uschamber.com/IoT-security

- *National IoT Strategy Dialogue* (Oct. 2017)—ITI, C_TEC, et al.

www.itic.org/public-policy/IoTReportFinal2.pdf

IoT Cyber Policy

Matthew J. Eggers (meggers@uschamber.com)

A Chamber statement accompanying these slides is available on this NIST website:

www.nist.gov/programs-projects/nist-cybersecurity-iot-program

Statement of the U.S. Chamber of Commerce

ON: Internet of Things (IoT) Cybersecurity Policy

TO: National Institute of Standards and Technology,
IoT Cybersecurity Colloquium

DATE: October 19, 2017

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
Executive Director, Cybersecurity Policy, U.S. Chamber of Commerce
National Institute of Standards and Technology
Internet of Things (IoT) Cybersecurity Policy
IoT Cybersecurity Colloquium
October 19, 2017

Good afternoon, my name is Matthew Eggers, and I am the executive director of cybersecurity policy with the U.S. Chamber's National Security and Emergency Preparedness Department. On behalf of the Chamber, I appreciate the opportunity to present our views on Internet of Things (IoT) cybersecurity policy.[1] The Chamber welcomes the National Institute of Standards and Technology's (NIST's) IoT cybersecurity program, which supports the development and application of standards, guidelines, and related tools to strengthen the security and resilience of connected devices and their associated operating environments.[2]

The Chamber's National Security and Emergency Preparedness Department was established in 2003 to develop and implement the Chamber's homeland and national security policies. The department'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 handle Internet of Things (IoT) issues, including our Chamber Technology Engagement Center (C_TEC) and Global Information Security Working Group (GISWG). First, C_TEC is at the forefront of advancing IoT deployment and innovation in the digital economy.[3] Among its initiatives are working groups on unmanned aerial vehicles, IoT, and autonomous vehicles.[4]

Second, the GISWG pushes the Chamber's views to international audiences, including calling on countries and regions to align their cybersecurity governance programs with the joint industry-National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (the framework). It also urges the protected sharing of cyber threat data among multiple public and private parties.

The GISWG and six European organizations recently 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.[5] Underpinning the Chamber's efforts at home and abroad is advocacy for smart policies for smart devices.

The Chamber's board of directors approved the principles and objectives in this paper in June 2017. They form the basis of the Chamber's July comments to the National Telecommunications and Information Administration (NTIA) regarding botnets and our recent testimony before a House subcommittee concerning the cybersecurity of the IoT.[6]

Summary: The Internet of Things (IoT) Will Further Economic Growth; Smart Risk Management Principles and Policies Are Fundamental to Sound Security

The U.S. Chamber of Commerce is 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. Indeed, 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. Fundamental cyber principles the Chamber will push to foster beneficial outcomes of the IoT are as follows:

- The IoT is incredibly complex, and there's no silver bullet to cybersecurity.
- Managing cyber risk across the internet and communications ecosystem is central to growing the IoT and increasing businesses' gains.
- The business community will promote policies favorable to the security and competitiveness of the digital ecosystem.
- IoT cybersecurity is best when it's embedded in global and industry-driven standards.
- Public-private collaboration needs to advance industry interests.

Overview: The Rapidly Emerging IoT Is Composed of Physical Things and Services

Descriptions of the IoT vary across stakeholders, yet the IoT generally refers to networks of objects that communicate with other objects and with computers through the internet.[7] The things may include virtually any object (e.g., a motion sensor) for which remote communication, data collection, or control may be useful—including vehicles, appliances, medical devices, electric grids, transportation infrastructure, manufacturing equipment, and agricultural systems. The emerging IoT may also more broadly affect economic growth, infrastructure and cities, and individual consumers.

To be sure, the IoT is more than just physical things. It includes services (e.g., smartphone applications) that support and depend on devices, as well as the connections among the devices, networks, and systems. In other words, the IoT potentially involves vast numbers and types of interconnections between objects and systems. It is widely considered the next major stage in the evolution of cyberspace.[8]

The Chamber views the IoT as composed of two major segments—consumer IoT and industrial IoT.[9] There is also a distinction emerging between managed and unmanaged IoT, in

which some IoT services and devices are consumer deployed, while others are part of value-added services and products administered by third-party providers (e.g., cloud-based platforms).

The Chamber believes the revolutionary benefits of the IoT will be realized only in an environment that prioritizes specific activities by industry and government, particularly managing cyber risk and avoiding regulations that would stunt IoT innovation and deployments.[10] The federal government, led by the Department of Commerce, should strive toward public-private collaboration, interagency coordination, and global engagement, especially with respect to standardization.[11]

The IoT is incredibly complex, and there's no one-size-fits-all solution to cybersecurity. The myriad, fast-moving threats that seek to compromise the IoT are borderless and include nation-states, organized crime, hacktivists, and terrorists that businesses cannot tackle alone.

Managing Risk Across the Internet and Communications Ecosystem Is Key to Growing the IoT and Increasing Businesses' Gains

Many companies go to great lengths to incorporate security into the design phase of IoT devices and services they sell globally. 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 leveraging sound risk management approaches in diverse settings such as manufacturing, transportation, energy, and health care.

Strong IoT security should be a win-win proposition for makers, providers, and purchasers.[12] Indeed, the IoT could dramatically unleash significant economic growth across the country and the world. According to a frequently cited report, approximately 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. By other accounts, the IoT could have a cumulative economic impact of $3.9 trillion to $11 trillion per year by 2025.[13]

Sound private sector-led IoT risk management initiatives can create a virtuous cycle of security in which consumers seek out secure devices and services, and industry stakeholders prioritize security in the design, production, and improvement phases of their offerings. Different sets of flexible cybersecurity best practices will be relevant for different IoT audiences, ranging from producers to network operators to users.

The Chamber, which has members operating throughout the entire IoT landscape, urges IoT stakeholders to mitigate risks in this technological environment so that hazards to businesses' cybersecurity do not pool at any given point. Unmitigated risk and threats could create perils not only for companies and sectors but for the IoT at large.[14]

To be sure, the private sector is not standing still in the face of increased risk from the IoT. A Gartner report says, "Worldwide spending on [IoT] security will reach $348 million in 2016, a 23.7% increase from 2015 spending of $281.5 million. In addition, spending on IoT security is expected to reach $547 million in 2018.[15] By 2020, Gartner predicts that over half of all IoT implementations will use some form of cloud-based security service.

Solutions are being developed and offered globally. As a leading cybersecurity company explains, security architectures are being refined to support comprehensive security because "IoT systems are often highly complex, requiring end-to-end security solutions that span cloud and connectivity layers, and support resource-constrained IoT devices that often aren't powerful enough to support traditional security solutions."[16] Increased attention is being paid to authentication and encryption. All of these measurers will improve security in the IoT, and it is vital that these innovations have a global reach.

Industry Will Promote Policies Favorable to the Security and Competitiveness of the Digital Ecosystem

Regulatory relief and reform are at the top of the Chamber's 2017 growth agenda. Businesses cannot expand and create jobs if they are burdened by complex and expensive regulations.[17] The vast potential of the IoT will be realized only in a hospitable policy climate. The explosive growth of the internet in the 1990s resulted from a minimal regulatory environment, which has been the foundation for U.S. global internet leadership.

Today, leading industry stakeholders are more attuned to the importance that cybersecurity brings to the marketplace.[18] While perfect security of network-connected devices is ambitious, the Chamber urges all stakeholders to make the cybersecurity of the IoT a priority—not simply for security's own sake but for the end-to-end well-being of the IoT ecosystem.[19]

The Chamber believes IoT-specific mandates or guidance, including ones related to security and privacy, are unnecessary.[20] As with other areas of cybersecurity (e.g., critical infrastructure), prescriptive legislation and regulations will have negative consequences on businesses and consumers. For example, IoT-related security mandates will slow innovation and quickly become obsolete compared with threat actors that can circumvent compliance-based regimes. The Chamber will push back against governmental actions that attempt to restrict a rapidly evolving field like the IoT.[21]

Further, overlapping and/or conflicting red tape at the federal, state, and local levels will impose unnecessary costs on businesses and erode the economies of scale needed for successful IoT penetration across the economy. So, too, fragmented national cybersecurity regimes will threaten important policy goals such as fostering the international interoperability of the internet and connected technologies and establishing meaningful information-sharing relationships among multiple public and private parties.

Maureen Ohlhausen, commissioner of the Federal Trade Commission, put it well when she said, "It is thus vital that government officials, like myself, approach new technologies with a dose of *regulatory humility* [italics added]."[22] In a similar vein, it's constructive that the FTC has said in its writings, "[T]here is great potential for innovation in this area, and that legislation aimed specifically at the IoT at this stage would be premature."[23]

Any policy effort needs to urge greater awareness by consumers about cybersecurity. Users will be a critical part of securing the IoT, given the swift pace of technical innovation and

the speed of IoT availability in the marketplace.[24] Buyers need to manage their devices, use passwords and other security-enhancing tools, accept provider updates, and be knowledgeable about connectivity security (e.g., Wi-Fi), among other cybersecurity basics.

IoT innovators are concerned about liability, which is a real threat and could negatively affect innovation.[25] Fears expressed by some about IoT security have been exploited by opportunists to target companies that make sound investments in the IoT. Such claims can lead to nonmeritorious lawsuits. For instance, certain vulnerability disclosures have led to class action suits, even when no unauthorized intrusion of a technology product or system occurred. And with the benefit of hindsight, alleged security issues can be the basis for unwarranted claims against industry regarding deception or unreasonable practices.[26]

Instead of pursuing punitive measures, policymakers should look for creative ways to reduce barriers to innovation and limit undue risk of liability to encourage desired information sharing, communication, and product development.

IoT Cybersecurity Is Best When Embedded in Global and Industry-Driven Standards

Cybersecurity standards and best practices are optimally led by the private sector and adopted on a voluntary basis. They are most effective when developed and recognized globally. Such an approach avoids burdening multinational enterprises and IoT adopters with the requirements of multiple, and often conflicting, jurisdictions.

Misplaced or unintended policy constraints will limit U.S. competitiveness in the global marketplace.[27] The Chamber welcomes the Department of Commerce's commitment to "advocate against attempts by governments to impose top-down, technology-specific 'solutions' to IoT standardization needs."[28]

International policymakers should align IoT security programs with industry-backed approaches to risk management, such as the framework. The framework is biased toward a standards- and technology-neutral approach to managing cyber risks. Moreover, policymakers need to support NIST's strategic engagement in international standardization to attain U.S. cyber objectives.[29]

Public-Private Collaboration Needs to Advance Industry Interests

Public-private partnerships are critical to addressing IoT cybersecurity.[30] Four examples highlight the importance of quality collaboration.[31] First, the NTIA's January 2017 *Green Paper: Fostering the Advancement of the Internet of Things* (the *Green Paper*) assesses what actions stakeholders should take to advance the IoT, including matters relating to cybersecurity.

The Chamber generally agrees with the agency's overall approach to public-private collaboration. "Over the past few decades in the United States," the NTIA observes, "[T]he role of government largely has been to establish and support an environment that allows technology to grow and thrive." Rather than intervening prematurely in the nascent, rapidly changing IoT marketplace, the NTIA's *Green Paper* stresses that the role of government is to establish and

support an environment that promotes the development and progress of emerging technologies by "[e]ncouraging private sector leadership in technology and standards development, and using a multistakeholder approach to policy making."[32]

Second, the NTIA is assembling a cybersecurity-focused multistakeholder process to address IoT security upgradability and patching of consumer devices that could prove helpful to interested parties. The Chamber believes the NTIA IoT security upgradability and patching effort and related activities can advance the private sector's interest in collaborative, voluntary best practices and shared information.

Third, NIST did an admirable job of convening many organizations to develop the framework. The Chamber believes the department is well positioned to convene stakeholders to identify existing standards and guidance to enhance the security and resilience of the IoT.[33]

Fourth, the Chamber recognizes the nonbinding principles the Department of Homeland Security put forward in its 2016 blueprint for securing the IoT across a range of design, manufacturing, and deployment activities. The Chamber looks forward to working with DHS leadership on improving the resilience of the IoT.[34]

***

The Chamber urges all stakeholders to play their parts to reduce risks associated with the growing IoT. Consumers need to demand secure devices and services. Companies that prioritize strong security should be rewarded through increased sales and market share. In addition, it is crucial that policymakers approach new IoT technologies with a dose of regulatory humility. There is abundant potential for innovation in this space. Legislation and other policies targeted specifically at the IoT could be detrimental to the creation of leading-edge products and services.

Endnotes

---

[1] www.nist.gov/news-events/events/2017/10/iot-cybersecurity-colloquium

[2] www.nist.gov/programs-projects/nist-cybersecurity-iot-program

[3] The Chamber Technology Engagement Center (C_TEC) strongly supports H.R. 686, the DIGIT Act. Adoption of this bipartisan legislation would be a critical first step in the public-private development of a national IoT strategy based on data and real-world experiences. The DIGIT Act would also bring together stakeholders in government and industry to shape policy, helping ensure that the U.S. realizes the full economic potential of IoT and remains a leader in this next chapter of the internet. www.congress.gov/bill/115th-congress/house-bill/686/cosponsors

On October 3, 2017, Intel, Samsung, the Information Technology Industry Council (ITI), the Semiconductor Industry Association (SIA), and C_TEC released the National IoT Strategy Dialogue, which advances recommendations to help Congress and the administration develop and foster policies to enable the U.S. to realize the vast economic and societal benefits of the IoT. www.itic.org/public-policy/IoTReportFinal2.pdf

www.itic.org/news-events/news-releases/technology-industry-leaders-release-national-strategy-to-maximize-u-s-economic-and-societal-benefits-from-the-internet-of-things

[4] www.uschamber.com/ctec

[5] See August 16, 2017, letter to European Commission from the American Chamber of Commerce to the European Union (AmCham EU), the Confederation of Danish Enterprise, the Confederation of Danish Industry, the Confederation of Industry of the Czech Republic, EurElectric, the International Chamber of Commerce in Belgium, and the U.S. Chamber of Commerce.
www.uschamber.com/sites/default/files/iot.cybersecurity.coalition._ec.letter.pdf

[6] On July 28, 2017, the Chamber submitted comments to the National Telecommunications and Information Administration's (NTIA's) notice on *Promoting Stakeholder Action Against Botnets and Other Automated Threats*.
www.ntia.doc.gov/files/ntia/publications/us_chamber_letter_botnets_iot_cybersecurity_final.pdf

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

http://plus.cq.com/doc/congressionaltranscripts-5191654?4

[7] 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

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

[9] 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

In March 2017, ITI wrote to the NTIA concerning the *Green Paper* and said the IoT encompasses consumer IoT and industrial IoT. Consumer IoT devices include household appliances, wearables, and smartphones; industrial IoT devices include factory equipment, building systems, and digital signage (pg. 2).
www.ntia.doc.gov/files/ntia/publications/iti.pdf

[10] See, especially, *The IoT Revolution and Our Digital Security: Principles for IoT Security*, September 19, 2017, written by the Chamber and Wiley Rein LLP. www.uschamber.com/IoT-security

NIST's "'Cybersecuring' the Internet of Things" (June 27, 2017).
www.nist.gov/blogs/taking-measure/cybersecuring-internet-things

[11] NTIA *Green Paper*, pgs. 11, 13.

[12] *2017 Cybersecurity Policy Priorities (Select Examples)*, Chamber's National Security and Emergency Preparedness Department (March 2017).
www.uschamber.com/sites/default/files/u.s._chamber_cyber_priorities_2017_short_version_final_march_2017.pdf

[13] www.ntia.doc.gov/files/ntia/publications/cati.iotcommentsfinal.pdf (pgs. 4–5)

[14] The Chamber's October 2016 *Statement on Encryption Policy and Cybersecurity* endorses robust encryption for information, including data at rest and data in motion.
www.uschamber.com/sites/default/files/documents/files/us_chamber_encryption-cyber_policy_statement_oct_14_2016_final_1_0.pdf

[15] *The IoT Revolution*, pg. 16; "Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016" (April 25, 2016). www.gartner.com/newsroom/id/3291817

[16] *The IoT Revolution*, pg. 16; Symantec, *An Internet of Things Reference Architecture* (2016). www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf

[17] Chamber's *2017 State of American Business Address* (January 11, 2017). www.uschamber.com/speech/2017-state-american-business-address

Chamber's *The State of American Business: Fixing Our Broken Regulatory Process* (February 13, 2017) www.uschamber.com/above-the-fold/the-state-american-business-fixing-our-broken-regulatory-process

[18] See, for example, IBM *Security's Five Indisputable Facts About IoT Security* (February 2017). www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEF03018USEN.

The Broadband Internet Technical Advisory Group *Internet of Things (IoT) Security and Privacy Recommendations* (November 2016). www.bitag.org/report-internet-of-things-security-privacy-recommendations.php

[19] The National Security Telecommunications Advisory Committee (NSTAC) found that "IoT adoption will increase in both speed and scope, and that it will impact virtually all sectors of our society. The Nation's challenge is ensuring that the IoT's adoption does not create undue risk. Additionally, the NSTAC determined that there is a small—and rapidly closing—window to ensure that IoT is adopted in a way that maximizes security and minimizes risk." The *NSTAC Report to the President on the Internet of Things* (November 19, 2014), pg. ES-1. www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf

Also see the opening statement of Rep. Fred Upton at a House Energy and Commerce joint Subcommittee on Commerce, Manufacturing, and Trade and Subcommittee on Communications and Technology hearing, "Understanding the Role of Connected Devices in Recent Cyber Attacks" (November 16, 2016). http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-MState-U000031-20161116.pdf

Cisco noted in its March 2017 letter to the NTIA on the *Green Paper*, "As we gain greater experience managing the risks and benefits of [IoT] technologies, governments should continue to *forbear from developing regulatory approaches* to the IoT marketplace [italics added]" (pg. 7). www.ntia.doc.gov/files/ntia/publications/cisco_ntia_supplemental_iot_comments_03_13_2017_final.pdf

[20] Comments of the staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning in response to the NTIA's April 2016 notice and request for comments, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (June 2016), pgs. 13–14. www.ntia.doc.gov/files/ntia/publications/p165403_ftc_staff_comment_before_ntia_in_docket_no_160331306-6306-01.pdf
www.ntia.doc.gov/files/ntia/publications/comments_of_c_tec_3-13-17.pdf

The IoT and cybersecurity do not raise novel privacy issues. The Chamber's comments on privacy are cited on pg. 31 of the NTIA *Green Paper*. We agree with ITI's March 2017 comments to the agency. ITI wrote that "a significant amount of IoT data will often have no connection to a person or individual. . . . [M]any of the privacy issues arising in the IoT context are nonetheless not new, as IoT applications where data on individuals is collected, the collection, use, sharing, and protection of such data are already subject to existing laws" (pgs. 4–5). www.ntia.doc.gov/files/ntia/publications/iti.pdf

[21] The NTIA *Green Paper* says, "Threats and vulnerabilities are constantly evolving. Predefined solutions quickly become obsolete or even provide bad actors with a roadmap for attack, the U.S. Chamber of Commerce noted. Many commenters stated that regulators must allow developers the flexibility to create cutting-edge improvements to defend their products and services and protect their users" (pg. 25).

In March 2017, USTelecom wrote to the NTIA on the *Green Paper* to say that the Department of Commerce and the NTIA "should encourage regulators to work with industry to identify potential cybersecurity gaps and distribute responsibilities across the broad ecosystem of device manufactures, applications developers, network service providers and others. Regulators . . . can *adopt more innovative and flexible means of collaboration* with industry [italics added]" (pg. 5). www.ntia.doc.gov/files/ntia/publications/ustelecom-comments-ntia-iot-2017-03-13-final.pdf

[22] Remarks of FTC Commissioner Maureen Ohlhausen, *Promoting an Internet of Inclusion: More Things AND More People, Consumer Electronics Show* (January 8, 2014), pgs. 1–2.
www.ftc.gov/sites/default/files/documents/public_statements/promoting-internet-inclusion-more-things-more-people/140107ces-iot.pdf
www.ntia.doc.gov/files/ntia/publications/cati.iotcommentsfinal.pdf

[23] FTC staff report, *Internet of Things: Privacy & Security in a Connected World* (January 2015), pgs. vii, 49.
www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[24] In its March 2017 comments to the NTIA regarding the *Green Paper*, Microsoft urged the Department of Commerce to acknowledge that basic cyber hygiene is a cybersecurity priority in the IoT space. "[M]any responsible technology providers ship patches on a regular basis, but users often fail to apply them," the company noted (pg. 5).
www.ntia.doc.gov/files/ntia/publications/microsoft_corporations_response_to_the_green_paper_-_march_2017.pdf

In its March 2017 letter to the NTIA pertaining to the *Green Paper*, Cisco noted the usefulness of the FTC's *Start with Security: A Guide for Business*, which distills practical lessons businesses can learn from the agency's casework on security.
www.ntia.doc.gov/files/ntia/publications/cisco_ntia_supplemental_iot_comments_03_13_2017_final.pdf

[25] In December 2016, the Commission on Enhancing National Cybersecurity's *Report on Securing and Growing the Digital Economy* called for the Department of Justice to lead an interagency study with the Department of Commerce and the Department of Homeland Security, among other agencies, and the private sector to "assess the current state of the law with regard to liability for harm caused by faulty IoT devices and provide recommendations within 180 days" (pg. 25).
www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

[26] In its March 2017 comments to NTIA on the *Green Paper*, the Security Industry Association said, "[T]here is a significant challenge not explicitly cited in the green paper—an uncertain or hostile legal environment that could deter IoT developers and limit the benefits of IoT devices for consumers. . . . IoT regulation by litigation is not a transparent or economically desirable policy solution to address concerns, and could be a serious impediment to growth and raise high-cost barriers to entry for small businesses" (pg. 3).
www.ntia.doc.gov/files/ntia/publications/iot_rpc_pt.2_sia.pdf

[27] "The knee-jerk reaction might be to regulate the Internet of Things, [but] . . . the question is whether we need a more holistic solution. *The United States can't regulate the world.* Standards applied to American-designed, American-manufactured, or American-sold device won't capture the millions of devices purchased by the billions of people around the world [italics added]."

This quote is taken from Rep. Greg Walden's opening remarks at a House Energy and Commerce joint Subcommittee on Commerce, Manufacturing, and Trade and Subcommittee on Communications and Technology hearing, "Understanding the Role of Connected Devices in Recent Cyber Attacks"
(November 16, 2016).
http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-MState-W000791-20161116.pdf

[28] NTIA *Green Paper*, pg. 13.

[29] Chamber letter to NIST, *Draft Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* (September 24, 2015).

www.uschamber.com/sites/default/files/september_24_2017_chamber_comments_draft_nistir_8074_intl_cyber_standardization_final.pdf

[30] In its March 2017 letter to the NTIA concerning the *Green Paper*, USTelecom wrote that it "supports the [Department of Commerce's] principle to convene stakeholders to address public policy challenges. In recent years, U.S. Government policy in an area of critical impact on IoT, namely cybersecurity, has been predicated on the assumption that a partnership between industry and government is superior to any prescriptive compliance regime, which, by its nature, would lack flexibility to respond promptly to new threats and potentially undermine security by providing the playbook for bad actors to exploit" (pg. 9).
www.ntia.doc.gov/files/ntia/publications/ustelecom-comments-ntia-iot-2017-03-13-final.pdf

[31] In its March 2017 comments to NTIA on the *Green Paper*, Samsung wrote, "[P]rivate sector leadership is critical to the success of the IoT in particular and technology growth and development in general. Yet collaboration between the government and private sector is essential to addressing challenges such as security and maintaining an open, global market for IoT technologies" (pg. 1).
www.ntia.doc.gov/files/ntia/publications/samsung_commerce-iot_comments_2017-03-13-c1.pdf

[32] NTIA *Green Paper*, pg. 2.

[33] In its March 2017 comments to the NTIA regarding the *Green Paper*, the American Cable Association said, "The NIST Cybersecurity Framework also provides a good model for the role of government in developing cybersecurity policies, as the Framework itself is the result of a highly collaborative effort between government and the private sector. While the government has a crucial role to play, it can be most helpful as a facilitator and convener—bringing together a diverse network of stakeholders to develop solutions" (pg. 5).
https://www.ntia.doc.gov/files/ntia/publications/aca.pdf

[34] The Department of Homeland Security's paper says these principles are intended for IoT developers, IoT manufactures, service providers, and industrial and business-level consumers. See *Strategic Principles for Securing the Internet of Things (IoT), Version 1.0* (November 15, 2016). www.dhs.gov/securingtheIoT