CYBERSECURITY OF THE INTERNET OF THINGS

HEARING

BEFORE THE

SUBCOMMITTEE ON
INFORMATION TECHNOLOGY

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

OCTOBER 3, 2017

Serial No. 115–40

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://oversight.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
27–760 PDF WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

Committee on Oversight and Government Reform

Trey Gowdy, South Carolina, *Chairman*

John J. Duncan, Jr., Tennessee
Darrell E. Issa, California
Jim Jordan, Ohio
Mark Sanford, South Carolina
Justin Amash, Michigan
Paul A. Gosar, Arizona
Scott DesJarlais, Tennessee
Trey Gowdy, South Carolina
Blake Farenthold, Texas
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Ron DeSantis, Florida
Dennis A. Ross, Florida
Mark Walker, North Carolina
Rod Blum, Iowa
Jody B. Hice, Georgia
Steve Russell, Oklahoma
Glenn Grothman, Wisconsin
Will Hurd, Texas
Gary J. Palmer, Alabama
James Comer, Kentucky
Paul Mitchell, Michigan
Greg Gianforte, Montana

Elijah E. Cummings, Maryland, *Ranking Minority Member*
Carolyn B. Maloney, New York
Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Stephen F. Lynch, Massachusetts
Jim Cooper, Tennessee
Gerald E. Connolly, Virginia
Robin L. Kelly, Illinois
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey
Stacey E. Plaskett, Virgin Islands
Val Butler Demings, Florida
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland
Peter Welch, Vermont
Matt Cartwright, Pennsylvania
Mark DeSaulnier, California
Jimmy Gomez, California

Sheria Clarke, *Staff Director*
Robert Borden, *Deputy Staff Director*
William McKenna *General Counsel*
Troy Stock, *Subcommittee Staff Director*
Kiley Bidelman, *Clerk*
David Rapallo, *Minority Staff Director*

Subcommittee on Information Technology

Will Hurd, Texas, *Chairman*

Paul Mitchell, Michigan, *Vice Chair*
Darrell E. Issa, California
Justin Amash, Michigan
Blake Farenthold, Texas
Steve Russell, Oklahoma

Robin L. Kelly, Illinois, *Ranking Minority Member*
Jamie Raskin, Maryland
Stephen F. Lynch, Masschusetts
Gerald E. Connolly, Virginia
Raja Krishnamoorthi, Illinois

CONTENTS

Page
Hearing held on October 3, 2017 1

WITNESSES

Mr. Matthew J. Eggers, Executive Director, Cybersecurity Policy, U.S. Chamber of Commerce
Oral Statement 2
Written Statement 5
Mr. Tommy Ross, Senior Director of Policy, The Software Alliance (BSA)
Oral Statement 18
Written Statement 21
Mr. Josh Corman, Director of the Cyber Statecraft Initiative, Atlantic Council
Oral Statement 30
Written Statement 32
Mr. Ray O'Farrell, Chief Technology Officer, VMware
Oral Statement 45
Written Statement 47

APPENDIX

Opening Statement of Representative Gerald E. Connolly 82
Questions for the record for Mr. Eggers, submitted by Chairman Hurd 84
Questions for the record for Mr. Ross, submitted by Chairman Hurd 89
Questions for the record for Mr. Corman, submitted by Chairman Hurd 92
Questions for the record for Mr. O'Farrell, submitted by Chairman Hurd 102

CYBERSECURITY OF THE INTERNET OF THINGS

Tuesday, October 3, 2017

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 2:19 p.m., in Room 2247, Rayburn House Office Building, Hon. Will Hurd [chairman of the subcommittee] presiding.

Present: Representatives Hurd, Mitchell, Issa, Amash, Gianforte, Kelly, Raskin, Connolly, and Krishnamoorthi.

Mr. HURD. The Subcommittee on Information Technology will come to order. And, without objection, the chair is authorized to declare a recess at any time.

The very first hearing we held in the subcommittee just over 2–1/2 years ago was titled, "Cybersecurity: The Evolving Nature of Threats Facing the Private Sector." Since that first hearing, we have held over a dozen hearings on a variety of cybersecurity issues facing the Congress and the country, including encryption technology, the risk posed by insecure legacy Federal IT systems, and the opportunities and challenges posed by connected vehicles.

Today's hearing on the Internet of Things builds on all the work we have done over the last 2–1/2 years to better understand the innovations of the digital age and how to implement needed legislative updates to continue protecting consumers and allowing American creativity to grow.

The Internet of Things presents an opportunity to improve and enhance nearly every aspect of our society, economy, and day-to-day lives. But in order for us to be able to fully harness this technology, the Internet of Things needs to be built with security in mind and not as an afterthought. When integrating these devices into our lives, people need to know that they are secure.

Unfortunately, we are far from this ideal state because many IoT devices violate basic cybersecurity practices. Some IoT devices lack the ability to be patched or include hard-coded passwords that cannot be changed by the user. This lateral vulnerability was explored in the recent attack on Dyn, which took down Netflix, Spotify, Twitter, and a number of other websites for hours.

Senators Mark Warner and Cory Gardner have recently proposed one way of potentially increasing the cybersecurity of these devices by introducing a bill that would set minimum security requirements for devices purchased by the Federal Government. I applaud them for the effort and the thought that went into this legislation.

I look forward to getting into the details of that legislation in today's hearing to answer some questions like, is the definition of IoT in the bill too broad? Does the bill apply to mobile devices? Should it? The cybersecurity requirements for devices in the bill might make sense now, but will they soon become outdated?

As I have said before, we have great challenges in front of us, but also a tremendous opportunity to be bold and decisive and reform the Federal Government. I thank the witnesses for being here today, and look forward to hearing and discussing bold ideas to increase the level of cybersecurity of the Internet of Things so that we can all benefit from the revolutionary opportunities it offers.

And as usual, I'm glad to be able to explore these issues with my friend and ranking member, the Honorable Robin Kelly from Illinois. And when she arrives, we'll recognize her for her opening remarks.

Mr. HURD. But we'll go ahead and make introductions of our witnesses. We have Mr. Matthew Eggers, the executive director for cybersecurity policy at the U.S. Chamber of Commerce; Mr. Tommy Ross, senior director of policy for the Business Software Alliance; Mr. Josh Corman, director of the Cyber Statecraft Initiative at the Atlantic Council; and Mr. Ray O'Farrell, chief technology officer at VMware. And welcome to you all.

And pursuant to committee rules, all witnesses will be sworn in before they testify, so please rise and raise your right hand.

Do you solemnly swear or affirm the testimony you're about to give is the truth, the whole truth, and nothing but the truth, so help you God?

Thank you.

The record will reflect all witnesses answered in the affirmative.

In order to allow time for discussion, please limit your testimony to 5 minutes. Your entire written statement will be made part of the record. And as a reminder, the clock in front of you shows your time remaining. And the light will turn yellow when you have 30 seconds left and red when your time is up.

And now I would like to recognize Mr. Eggers to give your opening remarks.

WITNESS TESTIMONIES

TESTIMONY OF MATTHEW J. EGGERS

Mr. EGGERS. Thank you, sir.

Good afternoon, Chairman Hurd, Ranking Member Kelly, and other distinguished members of the IT Subcommittee. My name is Matthew Eggers, and I'm the executive director of cybersecurity policy with the U.S. Chamber of Commerce. On behalf of the Chamber, I welcome the opportunity to testify before this subcommittee.

Let me begin by noting our appreciation for your support and leadership regarding the Modernizing Government Technology Act. Its passage is a top chamber of priority. I recognize that you're considering legislation comparable to S. 1691, The Internet of Things Cybersecurity Improvement Act of 2017. I've combined my statements to the Chamber's thinking on IoT and cyber.

The Chamber is optimistic about the future of IoT. Many observers predict that the connectivity of the IoT will bring positive benefits through enhanced efficiency and productivity across the economy. The Chamber is advancing roughly five principles to foster valuable outcomes in this area.

First, the IoT is complex, and there's no silver bullet to cybersecurity. The IoT includes both devices and services, such as sensors and smartphone apps. It is composed of two major segments: consumer IoT and industrial IoT. There's a distinction emerging between managed and unmanaged IoT. Some IoT services and devices are consumer deployed, while others are administered by third parties, like a cloud provider. The advantages of the IoT will be realized in an environment that prioritizes industry managing cyber risks and government avoiding regulations that would stunt IoT innovation and deployments.

Second, managing cyber risk across the internet in communications ecosystem is crucial to growing in the IoT and increasing businesses' gains. The Chamber wants device makers, service providers, and buyers to win from the business community leading the development of state of the art IoT technologies. Sound private sector-led IoT risk management can create a virtual cycle of security in which consumers demand secure devices and services and industry prioritizes security in their offerings. Different risk management practices will be relevant for different IoT audiences and situations.

Third, the business community will promote policies favorable to the security and competitiveness of the digital ecosystem. Businesses cannot expand to create jobs if they are burdened by complex and expensive regulations. Leading industry stakeholders are attuned the importance that cybersecurity brings to the marketplace. Perfect security of network-connected devices is ambitious, but the Chamber urges all stakeholders to make the cybersecurity of the IoT a priority, not simply for security's own sake, but for the IoT ecosystem as a whole. It is crucial that policymakers approach new technologies with a dose of regulatory humility.

Fourth, IoT cybersecurity is best when it's embedded in global and industry-driven standards. Cyber standards and guidance 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 averts burdening multinational enterprises in IoT adopters with the requirements of multiple and often conflicting jurisdictions.

Fifth, public-private collaboration needs to advance industry interests. Two examples are worth highlighting. One, the NTIA. The telecom and information arm of the Commerce Department is working with businesses to assess what actions stakeholders should take to advance the IoT, including cyber. The agency is leading a multistakeholder process to address IoT security upgradability and patching of consumer devices.

Two, missed, the department's standards body did an admiral job of convening many organizations to develop the popular cybersecurity framework, which was released in 2014, and the Chamber's built the national education campaign around it. The Chamber strongly believes the Commerce Department is well positioned to bring together stakeholders to identify existing standards and best practices to enhance the security and resilience of the IoT.

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

[Prepared statement of Mr. Eggers follows:]

Statement of the U.S. Chamber of Commerce

ON: Cybersecurity of the Internet of Things

**TO: House Oversight and Government Reform Committee
Information Technology Subcommittee**

DATE: October 3, 2017

1615 H Street NW | Washington, DC | 20062

The Chamber's mission is to advance human progress through an economic,
political, and social system based on individual freedom,
incentive, initiative, opportunity, and responsibility.

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
House Oversight and Government Reform Committee
Information Technology Subcommittee
Cybersecurity of the Internet of Things
October 3, 2017

Good afternoon, Chairman Hurd, Ranking Member Kelly, and other distinguished members of the Information Technology Subcommittee (subcommittee). 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 testify before the subcommittee regarding *Cybersecurity of the Internet of Things*. The Chamber welcomes the Subcommittee's dedication to examining leading cyber matters.

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.[1] Among its initiatives are working groups on unmanned aerial vehicles, IoT, and autonomous vehicles.[2]

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.[3] Underpinning the Chamber's efforts at home and abroad is advocacy for smart policies for smart devices.

I recognize that the Subcommittee is considering legislation comparable to S.1691, the IoT Cybersecurity Improvement Act of 2017. The Chamber is reviewing the legislation with our members and welcomes having a constructive dialogue with the subcommittee and its staff. Still, I will confine my written statement to the Chamber's thinking on the IoT and cybersecurity.

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.[4] 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.[5] 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.[6]

The Chamber views the IoT as composed of two major segments—consumer IoT and industrial IoT.[7] 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.[8] 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.[9]

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.[10] 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.[11]

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.[12]

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.[13] 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."[14] 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.[15] 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.[16] 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.[17]

The Chamber believes IoT-specific mandates or guidance, including ones related to security and privacy, are unnecessary.[18] 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.[19]

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]."[20] 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."[21]

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.[22] 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.[23] 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.[24]

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.[25] 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."[26]

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.[27]

Public-Private Collaboration Needs to Advance Industry Interests

Public-private partnerships are critical to addressing IoT cybersecurity.[28] Four examples highlight the importance of quality collaboration.[29] 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."[30]

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.[31]

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.[32]

***

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] 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

[2] www.uschamber.com/ctec

[3] 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

[4] 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

[5] 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

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

[7] 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, the Information Technology Industry Council (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

[8] 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

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

[10] *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

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

[12] 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

[13] *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

[14] *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

[15] 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

[16] 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

[17] 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

[18] 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

[19] 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

[20] 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

[21] 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

[22] 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

[23] 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

[24] 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

[25] "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

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

[27] 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

[28] 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

[29] 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

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

[31] 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

[32] 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

Mr. HURD. Thank you, Mr. Eggers.

And now it is an honor and indeed a pleasure to introduce my friend and our ranking member, the Honorable Robin Kelly from the great State of Illinois.

Ms. KELLY. Well, thank you, Mr. Chair.

Chairman Hurd, thank you for calling today's hearing, and thank you to our witnesses for being here today. We are here to talk about a critically important bill and the security of IoT devices that the Federal Government uses. Senators Warner and Gardner recently introduced S. 1691, the Internet of Things Cybersecurity Act, to help ensure that Federal agencies procure secure IoT devices. I have been working on the discussion draft of the companion bill. I want to thank the Senators for their continued leadership on this important cybersecurity issue.

IoT devices are incredibly helpful for American citizens, businesses, and our Federal Government. From drones to smart light bulbs to connected cars, hundreds of millions of Americans benefit from these devices every day. In fact, we expect to have more than 20 billion internet connected devices online by 2020.

Unfortunately, the high demand and lucrative market for IoT devices has also attracted bad actors who crank out cheap products that are insecure, unreliable, and vulnerable to malware. We all know the dangers posed by unsecured devices. Even the least tech savvy among us learned about the consequences last October when a distributed denial-of-service attack, or DDoS, attack on DNS service provider Dyn shut down internet access for millions on the East Coast. We learned that the attack was carried out by a bot that composed of thousands of compromised IoT devices. It was a sobering reminder that everyday appliances like web cams, smart TVs, and even thermostats can be turned into cyberweapons. There is no doubt that these attacks are growing in frequency and severity. The proliferation of IoT devices makes these attacks that much easier.

It is estimated that October's Dyn attack only used a fraction of the botnets' capabilities. We can only imagine the disruption that a larger cyber attack would cause. Lives are at stake in this matter. Given the gravity of this situation, Congress must be concerned about both disruptive cyber attacks and protecting sensitive data. Comprised devices can become access points for malicious actors to gain entry into the Federal Government's network.

S. 1691 and my draft companion bill bakes security into the procurement process. These bills ensure that procured devices meet minimum security requirements. We are talking about basic cyber hygiene, like ensuring that devices are patchable, that they do not contain known vulnerabilities or hard-coded passwords.

The legislation also provides agencies with flexibility to waive these requirements if they employ similar requirements or use third-party device certification standards. These requirements make our agencies more secure, while providing flexibility to vendors and agencies.

We cannot predict the future of technology, which is why my discussion draft also includes the creation of emerging technology's advisory board to review and provide recommendations to update guidelines in realtime to address emerging threats.

Importantly, these bills are not meant to provide extensive in-depth regulation. Sector-specific regulators will devise more precise rules to address the unique risks to each sector. Instead, they would establish minimal flexible standards for government procurement of IoT devices.

I've long said that the Federal Government must be a leader in cybersecurity. This legislation takes us closer to that goal, but my bill draft is not finished. We need the input of people like our witnesses, other stakeholders, and the public to make my bill as strong as possible so that our Federal agencies can be safe and secure. It is a fine line to walk to secure our IT systems while encouraging innovation. I hope that at the end of this process we have struck that perfect balance. I look forward to hearing the witnesses' ideas and contributions to strengthen this bill.

And again, thank you, Mr. Chairman.

Mr. HURD. I'd like to thank the ranking member. I always say that cybersecurity is one of the final remaining bipartisan issues in Washington, D.C.

Ms. KELLY. No. Have hope. No, there's more.

Mr. HURD. There we go. I like that. PMA, positive mental attitude.

So I'd like to now recognize Mr. Ross for your 5-minute opening remarks.

TESTIMONY OF TOMMY ROSS

Mr. ROSS. Chairman Hurd, Ranking Member Kelly, members of the subcommittee, it's a real honor for me to be here with you today. My name is Tommy Ross, and I'm here on behalf of BSA/The Software Alliance. With operations in over 60 countries around the world, BSA is the leading advocate for the global software industry, which contributes over 10 million American jobs and over a trillion dollars to the U.S. economy.

Our members are among the world's leading innovators of software and analytics capabilities that undergird the Internet of Things, or IoT. They are deeply invested in the success of the IoT because of its potential to transform and improve our lives. The Internet of Things is already generating new and improved business models and business processes in nearly every sector of the economy, from agriculture to cutting edge scientific research. And it's delivering unprecedented conveniences and opportunities to individual citizens.

At the core of the Internet of Things is the ability to analyze, process, and move data in novel ways. If we are to realize the tremendous potential of the IoT, we must secure that data against malicious cyber activity.

As the chairman said in his opening remarks, products must be developed with security in mind and not with security as an afterthought. For that reason, BSA's members are deeply committed to advancing strong cybersecurity throughout the IoT market. In fact, as we celebrate National Cybersecurity Awareness Month, BAS is launching a new cybersecurity policy agenda entitled, "Security in the Connected Age," and our agenda asserts cybersecurity for the Internet of Things as a high priority for policymakers. I've included a copy of this agenda in my written testimony.

Our agenda emphasizes five categories for policy development: promoting a secure software ecosystem, strengthening the government's approach to cybersecurity, driving international harmonization, developing a 21st century cyber workforce, and embracing emerging technologies to strengthen security.

Drawing on this agenda, I offer several principles in concrete policy recommendations for securing the IoT in my written testimony. In my time before you now I'd like to focus on three of those recommendations.

First, the calibrated approach to capturing the complexity of the Internet of Things will be essential to crafting effective IoT policies. IoT devices and the systems they support come with a broad range of characteristics, including widely varying levels of vulnerability and risk, a diversity of functions, and target markets of different types. An IoT-enabled pacemaker, for example, carries a much different set of risks than a connected toothbrush. Some devices, if compromised by malicious cyber activity, could pose direct risk to an individual's safety or the public health. Others are unlikely to cause physical damage, but could be commandeered by botnets, as the ranking member mentioned. Rather than a one-size-fits-all approach, we need a risk-based policy framework that accounts for these differences.

Second, IoT policies should build on existing software industry best practices. We should not treat the Internet of Things as some wholly new and unexplored realm demanding new and different policies. IoT devices are built around hardware and software that have been regular features of the technology landscape for years, even decades. In the software industry, the private sector and the government have worked closely over many years to develop a robust set of guidelines, best practices, and international standards for developing and sustaining secure software. As you consider cybersecurity in the IoT we should begin here.

Finally, effective IoT cybersecurity policies will recognize that the government has an important role, but it should be cautious in how it exercises its role to avoid interventions that will stunt the development of innovative products, including new cyber tools. In general, it should focus on convening and facilitating, rather than dictating solutions. The government can be most effective when it takes action to foster market-driven solutions, particularly those that can impact markets globally.

The government can play a critical role by driving multistakeholder processes to confront the most critical or most challenging questions and to seek to harmonize policy frameworks across sectors based on the outcomes of those multistakeholder processes.

Beyond that, though, the government must lead by example. As Ranking Member Kelly said in her opening remarks, the Federal Government must be a leader in cybersecurity. It must drive the market by demanding the most innovative security solutions private industry can provide and invest in emerging technologies that can reshape security architectures. Too often government acquisition is driven towards the lowest cost solutions rather than those that provide the best value. That must change.

In summary, we argue that policies for the Internet of Things will be most effective when they are risk-based rather than one-size-fits-all, when they build on existing best practices instead of reinventing the wheel, and when they facilitate collaboration between government and industry to tackle a shared challenge.

Thank you again for the opportunity to appear before you today. I look forward to your questions.

[Prepared statement of Mr. Ross follows:]

Testimony of Tommy Ross, BSA | The Software Alliance
Hearing on "Cybersecurity of the Internet of Things"
Before the IT Subcommittee of the House Committee
on Oversight and Government Reform
October 3, 2017

Chairman Hurd, Ranking Member Kelly, Members of the Subcommittee:

It is a great honor to appear before you today. My name is Tommy Ross, and I am here on behalf of BSA | The Software Alliance.[1] With operations in over 60 countries around the world, BSA is the leading advocate for the global software industry before governments and in the international marketplace.

Our members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. BSA's members provide software and other services that undergird the backbone of the Internet of Things (IoT). They are leading innovators in developing IoT applications, devices, and systems, and are global leaders in generating new approaches to securing the IoT.

I. Introduction

Along with other groundbreaking technological developments such as advanced data analytics and artificial intelligence, the IoT promises to transform how we live, both in our business operations and in our personal lives. The IoT comprises the growing network of "smart" devices that are embedded with Internet-connected sensors and leverage cloud-based analytics to transform the data produced by these sensors into actionable intelligence. It brings the tremendous economic and social power of "connectedness" that we have seen in computer and telecommunications devices to everyday appliances, vehicles, equipment, and even apparel. The IoT holds the potential to generate new and better business models and business processes in nearly every sector of the economy, from agriculture to cutting-edge scientific research, and to deliver unprecedented conveniences and opportunities to individual citizens.

At the core of the IOT is the ability to analyze, process, and move data in novel ways. If we are to realize the tremendous potential of the IoT, it is essential that we ensure the integrity, security, and freedom of these data flows. Meeting this obligation, in part, means establishing national and international policies that enable the free flow of data, including across borders. Policies to force data localization and inhibit

[1] BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Docusign, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens

cross-border data transfers — which are increasingly common around the world — pose a tremendous risk to the viability of the IoT.

Just as critical is the necessity of securing data transiting through the IoT. Because malicious cyber activity can prevent us from realizing the tremendous promise of the IoT, BSA's members share a commitment to advancing strong cybersecurity throughout the IoT market. In fact, as we prepare to celebrate National Cyber Security Awareness Month in October, BSA is launching a new cybersecurity policy agenda, entitled "Security in the Connected Age" (attached), and our agenda asserts cybersecurity for the IoT as a high priority for policymakers.

With more than half the world's population now online,[2] and as billions of devices are connecting to the Internet as part of the IoT,[3] cybersecurity has become paramount to the lives of individuals and the operations of businesses around the globe. As BSA's cybersecurity agenda states, malicious cyber actors threaten to "erode trust in the online environment, disrupt global commerce, and cause physical damage to critical infrastructure, ultimately putting lives at risk. To address this challenge to the connected economy, cybersecurity practices and tools must defend the integrity, privacy, and utility of the Internet ecosystem."

We are grateful to see the members of this subcommittee turning your attention to such a critically important issue. As you consider policies to best advance IoT cybersecurity, we would like to offer a few overarching principles upon which we believe such policies should be grounded, as well as several concrete policy recommendations.

II. Principles for IoT Cybersecurity Policymaking

First, ***a calibrated approach to capturing the complexity of the Internet of Things*** will be essential to crafting effective IoT policies. IoT devices and the systems they support come with a broad range of characteristics, including widely varying levels of vulnerability and risk, a diversity of technical architectures and functions, and target markets of different sizes and levels of sophistication.

The most common way for individuals to interact with the Internet remains through computers, smart phones, and other communications platforms. Yet, many IoT

[2] International Telecommunications Union, "World Telecommunication/ICT Indicators Database," 21st Edition, July 3, 2017. http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[3] Estimates of IoT devices to be connected to the Internet by 2020 have commonly ranged from 20 to 50 million. See "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," Gartner, Inc., November 10, 2015. http://www.gartner.com/newsroom/id/3165317. See also Evans, Dave, "The Internet of Things: How the Next Evolution of the Internet is Changing Everything," Cisco Systems, Inc., April 2011. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

devices operate in the background, collecting and transmitting data with limited human interface, while others control physical objects, such as vehicles or appliances. In addition, devices can often be differentiated by whether they are primarily intended for use by consumers or in the industrial sector, including in critical infrastructure. Furthermore, devices assume a wide variety of technical specifications: there are constrained devices and gateway devices; those with embedded operating systems and those without; and devices with wide variations in memory, computing power, and communications protocols. These differences are significant in crafting approaches to security.

Likewise, there is a wide range of risks associated with IoT devices. Some devices, if compromised by malicious cyber activity, could pose direct risks to an individual's safety or to public health; others are unlikely to have any effects in the physical world beyond ceasing to function. Yet, most IoT devices – though not all – can be used to facilitate damaging botnet attacks or other automated threats when compromised. Constructive IoT policies will consider and account for these differences.

These differences matter greatly for approaching IoT policymaking: we can all likely agree that far greater attention should be paid to the security and functionality of an IoT-enabled pacemaker than to an IoT salt-shaker (and yes, there is such a thing). Any approach to IoT policymaking that does not acknowledge and distinguish between this broad diversity of risk, functionality, and market characteristics, or that serves as the basis for one-size-fits-all approaches, will be ineffective and counterproductive, inevitably generating unintended policy outcomes. Instead, we encourage a definitional framework that facilitates the thoughtful application of security solutions tailored to address the most critical risks.

Second, policymakers seeking to address IoT cybersecurity should recognize the success of recent ***multi-stakeholder processes enabling industry-led solutions*** to pressing security challenges in the marketplace, and build upon this model. Notable among these recent initiatives are the National Institute for Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*[4] and the National Telecommunications Information Administration's processes addressing Internet of Things security and botnets.[5] These efforts have demonstrated that a

[4] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[5] The National Telecommunications & Information Administration has facilitated three relevant multi-stakeholder processes since 2016, addressing "Internet of Things Security Upgradability and Patching" (https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security); "Cybersecurity Vulnerabilities" (https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities); and "Promoting

collaborative approach between the government and the private sector that draws primarily on private sector expertise and leadership can yield meaningful results that broadly impact cybersecurity. Equally critical are global, open, transparent multi-stakeholder processes for international standards development.

Third, any policy approach to the IoT must be ***flexible and adaptable*** enough to continue to encourage change, innovation, and customization, but meaningful enough to raise the security bar. In our industry, not only do technologies constantly evolve; continued innovation is the *sine qua non* for a business's survival. Policies and regulations that become ossified over time, failing to account for or even stifling such innovation, can hamstring an industry that is central to the United States' unrivaled economic success. Nevertheless, BSA recognizes that flexibility and adaptability cannot become the foundation for *laissez-faire* governance that ignores real and growing cyber threats: rather, what we need are policies that can thoughtfully generate competition and innovation toward ever-higher security standards.

Finally, we encourage policymakers to craft policies with an eye toward ***international harmonization and interoperability*** as governments around the world are wrestling with the same challenges. IoT cybersecurity impacts both businesses and citizens around the globe, and the way other governments address the issue can substantially impact businesses and citizens in the United States. When governments take unique national approaches to securing the IoT, they often force businesses to develop country-specific product models or engaging in dozens of substantially different regulatory compliance processes; these outcomes can create enormous burdens on efficiency and product development costs. The U.S. has an opportunity to be a global leader toward international harmonization, as it has many times in the past, by adopting and advancing international standards wherever possible, supporting multi-lateral policy frameworks, and working with other governments to develop cooperative approaches to IoT security.

III. Policy Recommendations for IoT Cybersecurity

We hope the principles outlined in the preceding section will guide consideration of any policy relating to IoT cybersecurity. Let me turn now to some more specific policy recommendations.

(1) Develop a framework for managing IoT security according to risk. As previously noted, IoT devices vary vastly in technical architecture and function, prevalence, and risk. Effective IoT policies cannot treat them in a one-size-fits-all manner; instead,

Stakeholder Action Against Botnets and Other Automated Threats" (https://www.ntia.doc.gov/files/ntia/publications/fr_ntia_cyber_eo_rfc_-_rin_0660-xc035.pdf).

we must develop a framework for defining and categorizing IoT devices according to risk and technical variations, and build policy approaches around this framework.

As a preliminary sketch, for example, such a framework could be structured around four risk-based categories:

- Devices that, if compromised, could create a substantial risk to life safety or a massive economic disruption;
- Devices that, if compromised, could pose significant risk to personal privacy, including individual financial and identity data, or could create non-emergency public health hazards;
- Devices that pose minimal risk to public health, life safety, personal privacy, or the economy, but which could cause damage by being commandeered as part of a botnet or similar mass cyber event; and
- Devices that have such limited functionality as to pose minimal security risk.

This is an oversimplified sketch for illustrative purposes; additional categories and details would be necessary to capture the full diversity of risks, technical variations, and potential threat scenarios. Such a framework should consider not only risk, but also the intended and potential functions of a device, how prevalent it is (or is likely to be) in the market, and other relevant factors. As such a categorization is refined, it will allow policymakers to tailor policies to match risk, rather than painting this incredibly diverse and ever-changing array of products with the same broad and potentially damaging brush.

(2) Build on software industry best practices. We should not treat the IoT as some wholly new and unexplored realm demanding new and different policies. IoT devices are built around hardware and software that have been regular features of the technology landscape for years, even decades. In the software industry, the private sector and the government have worked closely over many years to develop a robust set of guidelines, best practices, and international standards for developing and sustaining secure software. As policymakers consider cybersecurity in the IoT, they would do well to begin here.

Best practices and international standards articulate guidelines for developing software according to security-by-design principles and a security development lifecycle that enables developers to build security measures into products from inception. These best practices and international standards address identity management, patchability/updatability, secure coding, supply chain management, vulnerability disclosure, and other key elements of a secure software ecosystem. While software security is not the *only* important element of IoT security, the deep reservoir of accumulated knowledge, experience, and best practices from the software industry should be a starting point for developing IoT security policies. We should build on this body of work rather than seeking to invent new standards, new regulations, or other new guidelines from scratch.

(3) Advance Tools to Communicate Critical Cybersecurity Information to Users. Standards and best practices for secure IoT devices are likely to be an important element of the cybersecurity solution; yet, another equally critical - and often ignored – element is promoting the adoption of secure products by both individual and enterprise consumers. As industry leaders in secure software practices, BSA welcomes competition on the basis of strong cybersecurity; however, too often, potential consumers lack the ability to make informed decisions that differentiate between products based on security, in part because there are few tools to enable consumers to obtain and compare critical product security information. We need such tools: mechanisms that help individual and enterprise consumers understand the security features and risks they would acquire with any given IoT device, and help users – particularly at the enterprise level – integrate IoT devices into networked systems in ways that maximize security.

(4) Promote Shared Responsibility for IoT Security. Stakeholders in the IoT are a broad and disparate group: software developers, hardware manufacturers, internet service providers, mobile communications platforms, cybersecurity services, makers of connected products ranging from household appliances to medical devices, and of course consumers. No single stakeholder can secure the IoT, and no single stakeholder should be held solely accountable for security the IoT. It is critical that we foster a policy environment and facilitate operational collaboration based on an ethic of shared responsibility.

In practice, an ethic of shared responsibility means that policymakers should avoid policies that seek to place the security burden on a single group of stakeholders. For example, while device manufacturers should unquestionably consider security as they develop products, equally important may be the security of the networks upon which those devices reside, or the security of the edge routers or gateway processors to which those devices connect. Effective security requires a systemic approach.

More than that, it means fostering collaborative approaches to security. For example, government-facilitated initiatives to bring together broad groups of stakeholders to combat botnets and other cyber threats resident on IoT devices have demonstrated their effectiveness in achieving consensus on means for collaboration, identifying voluntary best practices, and sharing lessons learned.[6] Likewise, some of the most effective operational campaigns to dismantle botnets have involved collaboration between a wide array of stakeholders, including BSA members, as well as other industry stakeholders, academic researchers, law

[6] For example, during its third session (2011-2013), the Communications Security, Reliability, and Interoperability Council (CSRIC), which is facilitated by the Federal Communications Commission (FCC), included a working group on "Botnet Remediation" that notably produced a "US Anti-Botnet Code of Conduct for Internet Service Providers" (https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-1). NTIA's current multi-stakeholder process on combatting botnets also shows promise in this regard.

enforcement agencies, and governments worldwide.[7] Policies that recognize the broadly shared responsibility for IoT security, and facilitate collaborative action across the community of stakeholders, will be most likely to advance meaningful security outcomes.

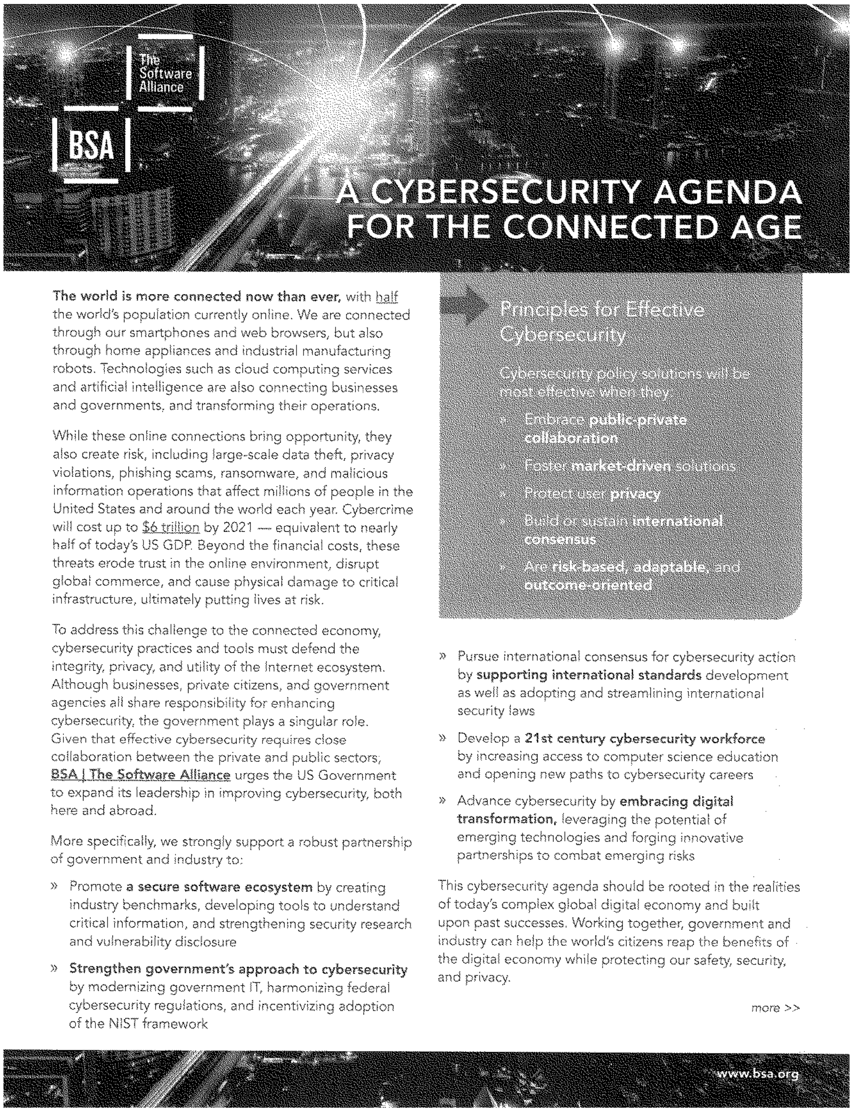
(5) Establish a Modest but Important Government Role. Finally, effective IoT cybersecurity policies will recognize that the government should have a role, but that it should be humble about its role. In general, it should focus on convening and facilitating, rather than dictating solutions. Fundamentally, the IoT represents a technology architecture spanning nearly all sectors of the global economy; for that reason, market-driven solutions are preferable because they will have a far greater impact than other approaches. Thus, the government can be most effective when it works to foster market-driven solutions, particularly those that can impact markets globally. The government can play a critical role by driving multi-stakeholder processes to confront the most critical or most challenging questions, and to seek to harmonize policy frameworks across sectors based upon the outcomes of these multi-stakeholder processes.

Beyond that, though, the government must lead by example. It must drive the market by demanding the most innovative security solutions private industry can provide, and investing in emerging technologies that can re-shape security architectures. Too often, government acquisition is driven toward the lowest-cost solutions, rather than those that provide the best value. That must change. In line with the principles articulated above, the government should demand that private industry compete to provide government institutions – and American taxpayers – with products that deliver both functionality and security, without being forced to cut corners on either priority simply to win lowest-price contracts. More generally, the government can leverage the power of its example to set market expectations for product security, foster innovation, and stoke competition for excellence.

* * * * *

Chairman Hurd, Ranking Member Kelly, and members of the Subcommittee, I am grateful for the opportunity to testify before you today. Security in the Internet of Things is a tremendously important concern, and our success in addressing it will underpin – or undermine – the foundation of the 21st Century economy. BSA and its members stand ready to be a key part of the solution, and look forward to working with you as you consider policy options to drive greater IoT security. Thank you for your consideration of our views.

[7] For example, the takedown of the "Avalanche" botnet, "one of the largest botnet takedowns ever," involved the collaboration of law enforcement agencies from over 30 countries, numerous private sector businesses, and the academic community. See Newman, Lily Hay, "It Took Four Years to Take Down 'Avalanche,' a Huge Online Crime Ring," *Wired*, December 2, 2016. https://www.wired.com/2016/12/took-4-years-take-avalanche-huge-online-crime-ring/.



The Software Alliance
BSA

A CYBERSECURITY AGENDA FOR THE CONNECTED AGE

The world is more connected now than ever, with half the world's population currently online. We are connected through our smartphones and web browsers, but also through home appliances and industrial manufacturing robots. Technologies such as cloud computing services and artificial intelligence are also connecting businesses and governments, and transforming their operations.

While these online connections bring opportunity, they also create risk, including large-scale data theft, privacy violations, phishing scams, ransomware, and malicious information operations that affect millions of people in the United States and around the world each year. Cybercrime will cost up to $6 trillion by 2021 — equivalent to nearly half of today's US GDP. Beyond the financial costs, these threats erode trust in the online environment, disrupt global commerce, and cause physical damage to critical infrastructure, ultimately putting lives at risk.

To address this challenge to the connected economy, cybersecurity practices and tools must defend the integrity, privacy, and utility of the Internet ecosystem. Although businesses, private citizens, and government agencies all share responsibility for enhancing cybersecurity, the government plays a singular role. Given that effective cybersecurity requires close collaboration between the private and public sectors, BSA | The Software Alliance urges the US Government to expand its leadership in improving cybersecurity, both here and abroad.

More specifically, we strongly support a robust partnership of government and industry to:

» Promote **a secure software ecosystem** by creating industry benchmarks, developing tools to understand critical information, and strengthening security research and vulnerability disclosure

» **Strengthen government's approach to cybersecurity** by modernizing government IT, harmonizing federal cybersecurity regulations, and incentivizing adoption of the NIST framework

» Pursue international consensus for cybersecurity action by **supporting international standards** development as well as adopting and streamlining international security laws

» Develop a **21st century cybersecurity workforce** by increasing access to computer science education and opening new paths to cybersecurity careers

» Advance cybersecurity by **embracing digital transformation,** leveraging the potential of emerging technologies and forging innovative partnerships to combat emerging risks

This cybersecurity agenda should be rooted in the realities of today's complex global digital economy and built upon past successes. Working together, government and industry can help the world's citizens reap the benefits of the digital economy while protecting our safety, security, and privacy.

Principles for Effective Cybersecurity

Cybersecurity policy solutions will be most effective when they:

» Embrace **public-private collaboration**

» Foster **market-driven** solutions

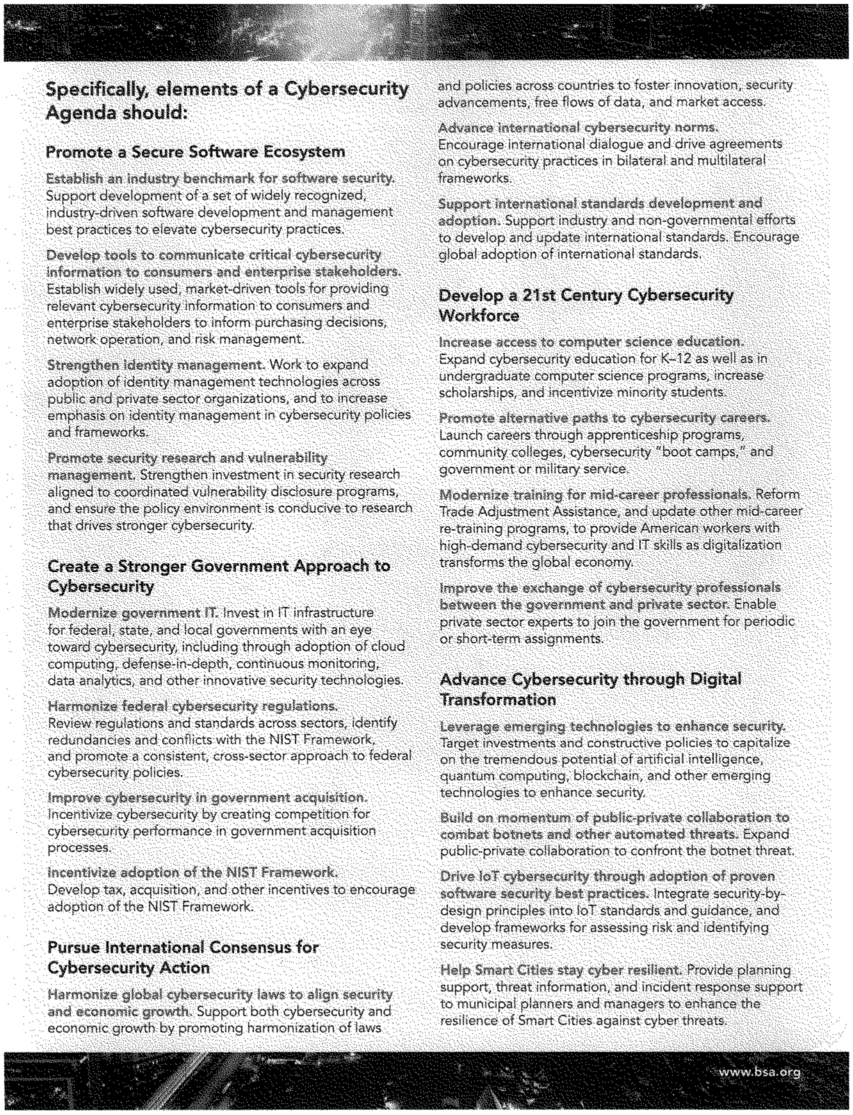
» Protect user **privacy**

» Build or sustain **international consensus**

» Are **risk-based, adaptable,** and **outcome-oriented**

more >>

www.bsa.org



Specifically, elements of a Cybersecurity Agenda should:

Promote a Secure Software Ecosystem

Establish an industry benchmark for software security. Support development of a set of widely recognized, industry-driven software development and management best practices to elevate cybersecurity practices.

Develop tools to communicate critical cybersecurity information to consumers and enterprise stakeholders. Establish widely used, market-driven tools for providing relevant cybersecurity information to consumers and enterprise stakeholders to inform purchasing decisions, network operation, and risk management.

Strengthen identity management. Work to expand adoption of identity management technologies across public and private sector organizations, and to increase emphasis on identity management in cybersecurity policies and frameworks.

Promote security research and vulnerability management. Strengthen investment in security research aligned to coordinated vulnerability disclosure programs, and ensure the policy environment is conducive to research that drives stronger cybersecurity.

Create a Stronger Government Approach to Cybersecurity

Modernize government IT. Invest in IT infrastructure for federal, state, and local governments with an eye toward cybersecurity, including through adoption of cloud computing, defense-in-depth, continuous monitoring, data analytics, and other innovative security technologies.

Harmonize federal cybersecurity regulations. Review regulations and standards across sectors, identify redundancies and conflicts with the NIST Framework, and promote a consistent, cross-sector approach to federal cybersecurity policies.

Improve cybersecurity in government acquisition. Incentivize cybersecurity by creating competition for cybersecurity performance in government acquisition processes.

Incentivize adoption of the NIST Framework. Develop tax, acquisition, and other incentives to encourage adoption of the NIST Framework.

Pursue International Consensus for Cybersecurity Action

Harmonize global cybersecurity laws to align security and economic growth. Support both cybersecurity and economic growth by promoting harmonization of laws and policies across countries to foster innovation, security advancements, free flows of data, and market access.

Advance international cybersecurity norms. Encourage international dialogue and drive agreements on cybersecurity practices in bilateral and multilateral frameworks.

Support international standards development and adoption. Support industry and non-governmental efforts to develop and update international standards. Encourage global adoption of international standards.

Develop a 21st Century Cybersecurity Workforce

Increase access to computer science education. Expand cybersecurity education for K–12 as well as in undergraduate computer science programs, increase scholarships, and incentivize minority students.

Promote alternative paths to cybersecurity careers. Launch careers through apprenticeship programs, community colleges, cybersecurity "boot camps," and government or military service.

Modernize training for mid-career professionals. Reform Trade Adjustment Assistance, and update other mid-career re-training programs, to provide American workers with high-demand cybersecurity and IT skills as digitalization transforms the global economy.

Improve the exchange of cybersecurity professionals between the government and private sector. Enable private sector experts to join the government for periodic or short-term assignments.

Advance Cybersecurity through Digital Transformation

Leverage emerging technologies to enhance security. Target investments and constructive policies to capitalize on the tremendous potential of artificial intelligence, quantum computing, blockchain, and other emerging technologies to enhance security.

Build on momentum of public-private collaboration to combat botnets and other automated threats. Expand public-private collaboration to confront the botnet threat.

Drive IoT cybersecurity through adoption of proven software security best practices. Integrate security-by-design principles into IoT standards and guidance, and develop frameworks for assessing risk and identifying security measures.

Help Smart Cities stay cyber resilient. Provide planning support, threat information, and incident response support to municipal planners and managers to enhance the resilience of Smart Cities against cyber threats.

www.bsa.org

Mr. HURD. Thank you, Mr. Ross.

Mr. Corman, you're up. Five minutes for your opening remarks. Thanks for being here.

TESTIMONY OF JOSH CORMAN

Mr. CORMAN. Thank you.

Chairman Hurd, Ranking Member Kelly, distinguished members of the committee, thank you for the opportunity to testify today. My name is Joshua Corman. I am a founder of iamthecavalry.org, a grassroots volunteer cyber safety initiative focused on where bits and bytes meet flesh and blood. Until yesterday I was the director of the Cyber Statecraft Initiative for the Atlantic Council, a nonprofit international policy think tank. And as of yesterday I am now the chief security officer for PTC to drive more maturity and safety into the industrial IoT sector. And lastly, relevant to today, I was testimony to the 2016 Presidential Commission for Enhancing National Cybersecurity and had the privilege of serving on the congressional task force for healthcare cybersecurity, which published in June.

Beyond my written testimony, I'd like to highlight three things. One is the cost of inaction and the urgency of time. While some want to wait, time really is the enemy here, and delayed response will have consequences in breaches; in effect, public safety; in the confidence in our government; and in very large parts of our economy, and could cede our leadership position in the international policy response after the next major attack in ways I fear through my work at the Atlantic Council would be very deleterious to U.S. interests and to our economic interests.

Number two, the Senate bill is promising because it focuses on an 80/20 rule type backbone of maximum benefit from minimum burden or on hovering around known vulnerabilities and reasonable cyber hygiene. These reasonable evergreen expectations both preserve and enable free market choice by definition. They are more descriptive than prescriptive, focusing on what is required versus how to do it, despite industry talking points. Further, they may even serve as a very necessary safe harbor rubric for inevitable software liability when we have our first casualties due to where bits and bytes meet flesh and blood.

And then third, this rubric could be made even better with a software bill of materials. Enhancing the Senate bill with a software ingredients list, or also referred to as a software bill of materials, would add significant protections and better reflect insights and findings from prior initiatives like the Presidential Commission, which highlighted the need for food labels and transparency to enable better free market choice; our healthcare Cybersecurity Task Force, which is strongly urging a software bill of materials to reflect what Philips Medical and others are voluntarily doing to make medical equipment safer in life critical use cases. And while the industry has reacted negatively to such approaches in the past, many of those arguments have been weak or have failed to fully appreciate the benefits of such an approach, both of which I'd be happy to speak to in Q&A or followup.

Further, we continue to misidentify as a Nation, especially when talking about the NIST cybersecurity framework, that cybersecurity is not only about confidentiality of data. It is about public safety, human life, capital expenditures, physical harm. And I think what we're seeing with NotPetya and other attacks is property damage, severe interruptions to our supply of vaccines for a national supply, et cetera.

And while I appreciate, especially from the technology community, the need—the reluctance to regulate technology, it's hard to argue that private sector is doing a good job here even on the regulation of data. About 100 of the Fortune 100 have lost intellectual property and trade secrets. Nearly every retailer has had a breach of credit card data several times, despite adhering to industry best practices, and I think the fact that we have a broad history of software security practices is part of the problem. We have failed secure low consequence use cases like replaceable data, and now we're increasingly dependent upon technologies where the consequences of failure could have a national security or public safety impact.

The breaches are getting bigger, like Ashley Madison and Target. They're affecting government, like the Pentagon and the OPM breach. And now they're affecting hospitals. Initially, last February, with Hollywood Presbyterian shutting down patient care for a week due to an accidental ransomware infection, and more recently, 65 hospitals in the U.K., 65 hospitals in one day were shut down, and it was 20 percent of their national capacity.

And while we have been reluctant, the primary reason to be reluctant to regulate software IoT, including my own reluctance, has been a fear that doing so may stifle innovation or hurt the economy. And I think these uncomfortable truths are showing a failure to have some reasonable regulation of software and IoT is stifling innovation and hurting the economy.

If we are cavalier about this, I do fear the international response. There's severe appetite to do things in Germany, in the U.K., and there are even attempts to break up the free open internet to have a U.N. takeover of governments. And the easiest solutions, the next Mirai botnet that we can't stop, are very dangerous to U.S. interests and may cede our current model and economic engagement with the internet.

Lastly, on a personal level, I'm very encouraged to see the enthusiastic support for the value of white hat research in coordinated vulnerability disclosure, and there's been significant strides there, which are already bearing fruit for the voting hacking machines, for medical devices, and for automobiles, and I'd like to see that continue. I'd be happy to answer your questions.

In closing, time is the enemy. The bill focuses on maximum benefit for minimum burden, and could be even strong with a bill of materials. I am encouraged by this hearing and the bill as a turning point that we might have the courage and will to do the technical solutions we've had available. Thank you.

[Prepared statement of Mr. Corman follows:]

Statement of Joshua Corman

For the House Oversight and Government Reform Committee's Subcommittee on Information Technology
"Cybersecurity of the Internet of Things"

Oct 03, 2017

Opening:
Chairman Hurd, Ranking Member Kelly, and distinguished Members of the Subcommittee on Information Technology, thank you for the opportunity to testify today.

My name is Joshua Corman. At the time of writing this, I am the Director for the Cyber Statecraft Initiative in the Brent Scowcroft Center on International Security at the Atlantic Council – a non-partisan, international policy think tank. I am a Founder of "I am The Cavalry" (dot org) a grass roots, volunteer, cyber safety initiative focused on public safety and human life in the internet of things – or as we like to say: "where Bits & Bytes meet Flesh & Blood". Additionally, I am an adjunct faculty for CISO Certificate Program at Carnegie Mellon University's Heinz College where I've worked with dozens of CISOs at a time. Lastly, I testified to the *2016 Presidential Commission on Enhancing National Cybersecurity* and served on the *Health Care Industry Cybersecurity Task Force* – initiated by Congress in the Cybersecurity Act of 2015.

Over the past 16 years, I've been a staunch advocate for the role of CISO (Chief Information Security Officer) – an increasingly difficult role. A significant portion of my research and career has been focused on the vanguard of emerging threats, and challenges affecting cybersecurity as well as identifying, advancing, and originating new and more effective responses to these growing challenges. As such, I've worked deeply with many of the Fortune 50, 100, and 1000 – on emerging issues such as the rise of cybercrime, the rise of nation state espionage, the rise of Anonymous & hacktivism, the Cyber Caliphate, and the growing exposures to cyber safety and national security as we become increasingly dependent on the Internet of Things.

As we continue to misidentify cybersecurity as primarily about the confidentiality of data, we grossly underestimate the urgency the situation commands. Over the last 2 years we are trending toward high consequence failures – well beyond data. As the most connected nation, we stand the most to lose.

Through our over dependence on undependable IT, we have created the conditions such that the actions of any single outlier can have a profound and asymmetric impact on human life, economic, and national security.

"I am The Cavalry" created this over-simplified list of material differences across the various types of IoT. Differences in:

- *Adversaries*: Motivations, Objectives, Capabilities, Will
- *Consequences of Failure*: Life & Limb, Physical Damage, Market Stability, GDP, International and National Security
- *Context & Environments*: Operational differences, Migratory, Perimeter-less, Inaccessible, Difficult to Patch/Replace
- *Composition of Goods*: Hardware, Firmware, Software
- *Economics*: Margins, Buyers, Investors, Costs of Goods, Regulatory, Depreciation
- *Time Scales*: Time-to-Live (TTL), R&D Cycles, Response Times

It is worth noting that Cybersecurity is a relatively nascent field – and is having a very difficult time rising to meet the challenges. High profile failures in the private sector and in governments are becoming quite clear. About 100 of the Fortune 100 have lost intellectual property or trade secrets to foreign industrial and nation state adversaries. Most Merchants have had a breach of credit cards – despite being compliant with "best practices" and industry compliance regulations like PCI DSS (Payment Card Industry Data Security Standard). Breaches are getting bigger like Target and Ashely Madison. Breaches are hitting Federal Agencies like the Pentagon and OPM. Breaches are getting dangerous as we connect everything in the Internet of Things – such as the denial of patient care at Hollywood Presbyterian Hospital in California due to Ransomware. WannaCry took out 65 UK hospitals – the US got VERY lucky. NotPetya hundreds of millions of dollars of damage to Mersk, Merck, and others. The Internet of Things is where bits & bytes now meet flesh & blood. In fact, the problem statement which caused me to form "I am The Cavalry" was:

"Our dependence on connected technology is growing faster than our ability to secure it – in areas affecting public safety and human life."

As society (and the government) increasingly depends upon IT, the importance of effective cybersecurity must also rise in kind. In the case of HHS, the consequences of failure may bleed into public safety and human life. We must be at our best.

"There are things the Public Sector ***can't*** *do, and the Private Sector* ***won't*** *do... and this is the role of Philanthropy and Altruism."*

– Eli Sugarman, Hewlett Foundation

As that 3rd category, I'm can say this issue has fallen through the cracks of the "Public Private Partnership" model.

Over the last 30 years, we have been *reluctant to regulate* software and IT. There are a number of concerns that have fueled this – some valid, some now less so, and some never were. The chief concern has been a fear that such actions might "Stifle innovation and hurt the economy." Attacks like Mirai launched from the long tail of low cost, low hygiene IoT device showed us that a *failure to regulate* IT can "stifle innovation and hurt the economy".

Since Mirai, we've seen significant damage to safety critical systems in the devastating impacts of WannaCry and NotPetya. A known but unmitigated vulnerability enabled WannaCry to take out 65 UK hospitals in a single day (20% of their national capacity of trusts) and affect manufacturing and other industries. NotPetya did material harm to Mersk shipping affecting the Port of LA, and Merck affecting their public earnings and having a material impact on their production of vaccines – like Hepatitis-C. Healthcare alone affects one sixth of our economy. Any crisis of confidence in the public could materially affect our economy. Any avoidable or elective shortfalls of our national supply of pandemic vaccines, the availability of life saving service during a natural disaster or domestic attack, or significant interruptions to critical infrastructure... could be devastating to our national interest.

What Mirai revealed:

DDoS attacks from the Mirai botnet took out the Internet for a good chunk of a Friday – affecting eCommerce, access to Netflix, CNN, Spotify, and other web services. It levied what was (at the time), the largest flood of traffic in history – at around a Terabit per second. Worse, only a fraction of the full botnet was leveraged in this attack – and those nodes participating only used a fraction of their possible sending capacity. At the time, I referred to Mirai as an IoT Tsunami of our technical and security debt catching up with us. The growing number of low cost, low hygiene IoT devices on the internet represents a public health issue for a reliable and sustainable Internet.

On a technical level, 3 things enabled Mirai to be so bad. These devices:

1. Were Internet reachable
2. Had guessable credentials (username & password) [and in this case fixed]
3. Were un-patchable

This combination is not isolated to the (majority) Internet Cameras. These said same 3 attributes apply to far too many medical devices – including $500,000 imaging equipment and devices that may directly harm patients. The next Mirai-like botnet could both target incredibly vulnerable hospitals to cause a denial of patient care – or actually be *comprised of* unfixable medical devices. Other, legacy critical infrastructure shares such attributes in Oil & Gas, Power, Water, and other designated US Critical Infrastructure

Uncomfortable truths command uncomfortable responses. If we want to see something different, we need to incentivize something different.

We have technical solutions for many of our exposures. What we have previously lacked is motivation and will. I am hopeful that the Senate Bill and this hearing are signs this is changing.

From a policy perspective, Mirai disrupted the "prior prevailing hopes" with regards to lighter touch regulation/policy. Prior discussions were focused on the belief that adding transparency, security "nutrition labels", and a software bill of materials (or ingredients list) that would enable consumers and purchasers to better discern "more secure products" from "less secure products". The bulk of discussion was about enabling free market choice. Mira revealed the externalities challenges and Tragedy of the Commons aspects of our inter-dependence. While transparency can allow each of us here today to buy a safer product, choices made *by others* can still hurt us – severely.

As someone *from* the Software, IT sector, and security research community, my natural preference to let the free market regulate itself – where informed, self-interested "demand", meets sufficient "supply". The 2 main areas where free markets – on their own – tend to need help are when there is either:

1. "Information Asymmetry" - where buyers lack enough information to act in their own self-interest, or

2. the rarer, "Tragedy of the Commons" – where even if each of us act in our own self-interest and local optimums, the whole is harmed.

Mirai and other cybersecurity issues are showing us we have both. The general fix for Information Asymmetry is to require more labeling, information, and transparency – to be *descriptive*. The fixes for Tragedy of the Commons is often using either *ex ante* (prior to harm) more *prescriptive* "what to do" requirements, or *Ex Post* (after harm) liability for outcomes – without prescribing *how* to avoid said outcomes. The rate of change in IT make *ex ante* too brittle to have efficacy over time and are more likely to stifle innovation or introduce barriers to entry for smaller players (or new entrants).

On S. 1691:

Initial exploration of what became Senate Bill 1691 appears to have followed the uncomfortable truths revealed by Mirai – and continued to evolve in the face of other critical mass in the policy community (see Critical Mass section below).

In broad brushstrokes, it is a technically grounded set of evergreen "Cyber Hygiene" principles that should be reasonable, achievable, and effective for classes of accidents and adversaries. High intent, high capability adversaries will remain an issue, but these principles should significantly raise the bar.

NOTE: The senate bill alone will not prevent the next Mirai. I believe they know that. Nor are large scale IoT denial of service attacks the only risk. Poor hygiene IoT could be at the root cause of the next OPM or Pentagon breach – or attempts to surveil or compromise your own Congressional offices via your Smart Television or Smart Gadget (for example).

These procurement guidelines may set an example for the private sector to adopt broadly, and/or a Self-Regulatory Organization, and/or international response (See International section below). In the face of a high consequence failure, I would not be surprised to see case law or introduction of software liability – and this rubric could inform and contribute to something like "safe harbor conditions" around "known vulnerabilities".

On Known Vulnerabilities:

All software has flaws and nearly no software will ever be without vulnerabilities (in any scalable, economic way) so we have to prioritize. "Known vulnerabilities" are a key chunk of an 80/20 Pareto Principle here. Known Vulnerabilities are significantly more likely to be exploited than unknown ones. For example, the vulnerability is BASH that enable ShellShock had been there for 2 years, but was not attacked (broadly) until discovered. Once a vulnerability is known, there is a gold rush effect (or a shark frenzy with blood in the water) where adversaries and defenders create methods of finding and exploiting them – fairly quickly.

Broadly speaking, the talent required to *find* a new vulnerability can often be high. The talent required to *create a reliable exploitation* of vulnerability can also be high. Once an attack tool is created and shared, using these tools can be *executed by nearly anyone*. In the spirit of Moore's Law (describing the growth rate of computing power), I once coined a term called "HDMoore's Law" – in that the strength of an unskilled adversary grows at the rate of the Metasploit Project (a free open source attack tool used by defenders – created by security researcher: H.D. Moore). Later, a data scientist Michael Roytman showed how a Known Vulnerability CVE (Common Vulnerability and Exposure) in both Metasploit and the ExploitDB was 30 times more likely to be attacked than one that wasn't.

Further, it is far more reasonable to expect vendors to be responsible for avoiding or remediating known vulnerabilities than the bevvy of as-of-yet unknown, potential ones. In the case of 3rd party and open source libraries (which can be north of 90% of modern software composition) the remediation is often done by those projects and the fix can be applied by the final goods assembler with significantly less effort than fixing their own custom, bespoke code.

Senate Bill 1691, by expecting products to be free of known vulnerabilities as a condition of procurement, dramatically reduces elective risk. By requiring these known vulnerabilities to at least be disclosed, informs/supports them to assess, factor, accept, shield those issue in their purchasing choices and their operational security throughout deployment. The current opaque model constitutes a "failure to warn."

One short fall of this bill is the omission of a software bill of materials – of all the 3rd party and open source libraries used in the product (including version numbers). There have been negative reactions from parts of the private sector to such proposals – some of which have merit, many of which are false. I could explain some of these upon request. There is limited adoption of this in the private sector, but they are proving it can be done and has value. E.g. Philips Medical is voluntarily publishing a Software Bill of Materials to their customers – and some other medical device makers are starting to. Not to mention the concept was pioneered by Deming at Toyota in the 40's – to drive efficiency and profitable manufacturing. Carrots & Sticks could be explored – as well as a timeline for enforcement.

Here are at least three use cases enabled by the inclusion of such a Software "ingredients list" (the likes of which are required by all food, for example):

1. At procurement time, buyer can tell better hygiene products from worse hygiene product and/or or factor the cost of aftermarket securing them in their deployment uses (currently covered by S. 1691)
2. For the life of the deployment, when a new vulnerability becomes known, they can immediately answer 2 questions
   a. "Am I affected?", and
   b. "Where am I affected?"

   especially when time is of the essence and patches may not be available (This could have helped avoid the Feb 2016 hospital outage at Hollywood Presbyterian Hospital – which was due to 1 Java flaw - in 1 JBOSS library in - 1 device – and they were warned about it, but didn't know what might use it)
3. Since companies go out of business, and product support expires, there will be no alert notification or security update ever coming – and this list is your only way to triage and react

On Patching & Security Updates:
After Mirai, I said "Unpatchable IoT are the lawn darts of the Internet" – in that they are inherently unsafe – "unsafe at any speed"... Since all software has flaws, and new vulnerabilities will be fund and exploited, robust, reliable, prompt and agile updates are going to be table stakes. With great connectivity, comes great responsibilities. One can no longer be hackable, but un-remediate-able.

Commerce NTIA's process on IoT Patching and Updates could be leveraged here.

On Avoiding Fixed Credentials:
This was a key factor in enabling Mirai. Sadly, this is quite a common practice. While initial default passwords and the ability to physically (or locally) reset them do have use cases, there are many established practices to avoid *keeping* these password after installation. The collective harm of the status quo is too high (even if localized risk is acceptable).

On Non-Deprecated / Standards Protocols and Crypto:
There is value here as well – as too many vendors try to be clever in effective ways – or use available but ineffective protocols, technologies, and encryption.

We would not want to stifle emerging, but as-of-yet not Standard innovations like the next Bluetooth. Perhaps, like disclosing known vulnerabilities, the bill could require non-standard or old technologies to be explicitly declared.

On Coordinated Vulnerability Disclosure and Safe Harbor for Good Faith Research:
Many in the security research community were pleased to see another acknowledgement of the value of good faith security research. Laws like DMCA and CFAA have had a significant chilling effect on security research – research which can have profound benefit to the manufacturer, their customers, the public good, and public safety. E.g. recent fixes to medical devices like:

- the Johnson & Johnson ANIMAS Insulin pump (found by Jay Radcliffe), or
- the bevvy of Voting Machine flaws found during this year's DEF CON hacking conference (attended by your own Chairman Hurd and Rep. Langevin) to help ensure the integrity of future elections.

In 2015 and 2016, "I am The Cavalry" and others supported no less than 18 US Government positive actions related to the value of coordinated vulnerability Disclosure. Those included, FDA guidance, DOT, DHS, DOD, Congress, NTIA, and more. Full list here:
https://www.iamthecavalry.org/usgdisclosure

As for the implementation, the "devil is in the details" of how this section plays out. I would encourage a few things as this section gets discussion, debate, and alteration:

- The current 3 year DMCA exemptions for good faith research on things like Voting Machines, Cars, Medical Devices, and Consumer Electronics are already showing fruit and proving the value of making them permanent. These significant discussions and stakeholders would be instructive both for DMCA and for possible mirroring for CFAA.
- The Librarian of Congress and Copyright Office has recommended they would like these exemptions to be made permanent. Congress could consider giving that recommendation the strength of law. If I recall, the FTC has also suggested this. I am not a lawyer, but law professor Andrea Matwyshyn (also now a Non-Resident Senior Fellow for me at Atlantic Council) was directly involved in these exemptions and has specific analysis regarding the current S. 1691 wording.
- The Commerce NTIA Multi-Stakeholder Process for Coordinated Vulnerability Disclosure also yielded a template, two surveys, and guidance for the harder, multi-party disclosures – and these materials and Executive branch leaders will have valuable insight.
- While the bill does call out ISO 29147 which outlines a standard for receiving and responding to disclosures, it would be more complete to include ISO 30111 for the process of triage and resolution
- We would want to ensure the discovery and/or research itself was protected – and not merely hinge on the act of disclosure.

On Alternative Approaches to S. 1691 – and the Geo-Political Context:
Were another Mirai or devastating attack to occur and trigger a knee-jerk, domestic or international policy response, there are other methods that could stop the attacks, but many are quite dangerous and have less obvious downside/risks. They may be worth exploring, but in a vacuum, I fear some of the fastest and easiest fixes may play into the hands of our adversaries and oppressive regimes. For example:

- Nation Centric Internet Sovereignty/Filtering – Via the UN/ITU: Russia, China, and some of the Middle East and African nations have tried to advocate for Balkanization of the Internet – away from the current Multi-Stakeholder Internet Governance Model. This can enable greater censorship, surveillance, dissident tracking/oppression, etc.

- Enable Carriers to do Deep Packet Inspection and Filtering: This could get entangled with Net Neutrality debates and current safe harbor from the transmission of illicit/illegal material
- Destroy or "Brick" the devices: Many proposed this after Mirai – and things like BrickerBot actually did destroy some devices. This has serious risks, could cause property damage, and while people thought it was less of an issue for cheap IoT cameras, think of the harm to medical devices and industrial systems. Further, some vulnerable components like BusyBox found in cheap IoT – are ALSO found in these safety critical devices like medical equipment – so you may aim to destroy camera and end up affecting human life or capital equipment destruction.

Other countries have been hit hard too... like Germany by Mirai and the UK by WannaCry. It is my belief that if the US does not lead here, we will end up being affected by European policy changes – and/or those pushed by our enemies. I see this as a foot race to decide what we want – and harmonize with our international allies.

Time is the enemy. The time for hand waving and hesitation is over. We should measure twice, cut once – and seek a basis of evergreen and internationally effective policies, but the status quo will not stand beyond the next high consequence attack.

Reaching Critical Mass:
"I am The Cavalry" has published simple frameworks for primitives and table stakes on Connected IoT Devices:

A "5 Star Cybersafety Framework for Connected Vehicles" and a "Hippocratic Oath for Connected Medical Devices" (linked below). Both essentially say... All systems fail. Therefore, you need to be ready for failure across 5 dimensions. Essentially, the guidance asks manufacturers to tell the market how they:

1. Avoid Failure (Safety by Design)
2. Take Help Avoiding Failure (Third Party Collaboration – Vulnerability Disclosure Programs)
3. Notice & Learn from Failure (Evidence Capture)
4. Respond Quickly to Failure (Security Updates)

5. Contain & Isolate Failure (Segmentation & Isolation - of Critical Systems from Non-Critical Systems)

AUTO
https://www.iamthecavalry.org/domains/automotive/5star/

MEDICAL:
https://www.iamthecavalry.org/domains/medical/oath/

In government, throughout 2016 and 2017, several Executive & Legislative policies & documents have been converging around a few key themes surrounding minimum Cyber Hygiene – to better insulate us from harm caused by accidents and adversaries:

Below are a few examples:

- 2017 Executive Order on Cybersecurity:
  - "for too long accepted antiquated and difficult-to-defend IT"
  - "commensurate with the risk and magnitude of the harm"
  - "Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies"
  - "attacks that could reasonably result in catastrophic regional or national effects on public health or safety"
  - "cybersecurity risks facing the defense industrial base, including its supply chain"
  - https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

- 2017 Congressional "Health Care Industry Cybersecurity Task Force"
  - Known Vulnerabilities Epidemic
  - Call for a required Software Bill of Materials or Medical Devices and Electronic Health Records Systems (EHR/EMR)
  - https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

- 2016 Presidential Commission on Enhancing National Cybersecurity
  - "Nutrition Labels" for IoT to enable consumer choice
  - An exploration for the state of the law regarding Liability with regards to software and IoT
  - https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

- 2016 US Commerce NTIA's Multi-Stakeholder Processes on:
    - Best Practices for Coordinated Vulnerability Disclosure
        - https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities
    - Upgradability and Patching for Internet of Things
- 2016 DHS Strategic Principles for Securing the Internet of Things
    - Security by Design
    - Patch-ability
    - Software Bill of Materials
    - Coordinated Vulnerability Disclosure Programs
    - https://www.dhs.gov/news/2016/11/15/dhs-releases-strategic-principles-securing-internet-things
- 2016 FDA Post-Market Guidance (and prior 2014 Pre-Market)
    - Patching / Security Updates
    - Promotion of (and Incentives for) Coordinated Vulnerability Disclosure Programs
- 2016 FTC "Start with Security" 10 Principles
    - https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

Mr. HURD. Thank you, Mr. Corman.

Mr. O'Farrell, you're now recognized for 5 minutes.

TESTIMONY OF RAY O'FARRELL

Mr. O'FARRELL. Chairman Hurd, Ranking Member Kelly, thank you for the opportunity to testify today at this important hearing. I am Ray O'Farrell, chief technology officer at VMware. I am head of VMware's IoT team. VMware is headquartered in Palo Alto, California, and is one of the largest software companies in the world, and is also part of the Dell Technology family of companies.

The emergence of IoT, or the Internet of Things, is a technological step in which more and more aspects of the physical world, from manufacturing to banking to home monitoring to healthcare, transportation, and even smart cities are interconnected and coupled with analytics and intelligence. Some consider the Internet of Things to be the basis of the next industrial revolution.

This level of IoT interconnect will lead to exciting new opportunities for American innovation and job growth. However, with the increased interconnect there is also a threat of cyber attack on this new infrastructure. We've already witnessed some of the security challenges for IoT. For example, just a year ago, an IoT distributed denial-of-service attack took down major internet platforms and disrupted the internet services of millions of Americans. And in May of this year, the WannaCry attack is estimated to have affected 100,000 organizations in 150 countries, and in the context of IoT, that included healthcare-related IoT systems. The threat and the impact of IoT-based cyber attack is not theoretical, it is real.

VMware is a leader in data center and IT infrastructure management, including the management of end-user devices such as cell phones. We do this for the Federal Government and the largest companies in the world. We extend this management and security approach to the world of IoT and to the IoT industry. We applaud Senators Warner and Gardner for introducing this proposal of the Internet of Things Cybersecurity Improvement Act of 2017, and the committee for releasing a discussion draft and holding today's hearings.

There are several provisions of the proposal that VMware specifically supports. Firstly, we believe that IoT devices should from the outset be designed with vulnerability patching capabilities built in.A simple patching requirement would have drastically reduced or eliminated the WannaCry breach.

Secondly, we support several of the cyber hygiene concepts in the proposal, including microsegmentation and multifactor authentication. The concept of microsegmentation plays a critical role in ensuring that IoT-related data and information are segmented and properly protected against IoT cyber breaches.

Thirdly, we also support the consideration included in the proposal that leverages security benefits introduced by properly managed IoT gateways, eight systems which act as isolation and management gateways to help prevent and remediate any compromise of connected devices.

In closing, the Internet of Things will have significant positive impact on American innovation and American jobs. Billions of IoT-connected devices will be on the free market for consumers, businesses, and government to consider purchasing. And the U.S. has a ripe opportunity to claim global leadership in this space. But security is the key principle that will enable and advance further adoption of IoT. If consumers, businesses, and government do not feel that IoT products are secure, it will only hinder U.S. global leadership in a growing and innovative IoT industry.

The Internet of Things Cybersecurity Improvement Act of 2017 provides a thoughtful framework modeled after the industry-recognized NIST framework. The specific proposal focuses narrowly and appropriately on the procurement process by the Federal Government of IoT technology. If the U.S. Government decides to spend American taxpayer dollars to gain the productivity and efficiency benefits that IoT technologies can bring to the government, then it is reasonable to assume that the government should be confident in the security levels of the IoT devices it is purchasing.

Chairman Hurd and Ranking Member Kelly, I applaud the leadership of the committee for holding this hearing today. Thank you for the opportunity to testify. And I look forward to answering the committee's questions.

[Prepared statement of Mr. O'Farrell follows:]

Testimony for the Record

Ray O'Farrell

Chief Technology Officer

VMware, Inc.

Before the

U.S. House of Representatives

Committee on Oversight and Governmental Reform Committee

"Cybersecurity of the Internet of Things"

October 3, 2017

Chairman Hurd, Ranking Member Kelly, and Members of the Committees, thank you for the opportunity to testify today at this important hearing. I am Ray O'Farrell, executive vice president and chief technology officer at VMware Inc; and head of VMware's Internet of Things business unit. I have nearly 30 years of experience in the software engineering field, primarily in embedded systems and secure, robust infrastructure software.

VMware is a leading provider of software-defined solutions that increase the operational efficiency and security of data centers within the federal government and across the globe. Currently, VMware is one of the largest software companies in the world with 2016 revenues of over $7 billion and more than 19,000 employees. We are headquartered in Silicon Valley, California, with 140 offices throughout the world, serving more than 75,000 partners and 500,000 customers, including 100 percent of the Fortune 500. The U.S. government is a long standing critical partner and customer of VMware and we remain committed to serving all sectors of the U.S. Government – including the Department of Defense, civilian agencies, and the Intelligence Community, as well as state and local governments. VMware is a part of the Dell Technologies family of companies, which is the largest privately controlled technology company in the world.

We are committed to providing both government and commercial organizations with the ability to respond to their dynamic business needs, whether they utilize on-premises datacenters, the cloud, or personal computers and mobile devices. VMware is providing enhanced security to government and commercial customers globally through its pioneering role in redefining how we build and secure networks, data centers, computers, and devices.

Cybersecurity Policy

The U.S. Government is dependent on a vast cyberworld of interconnected information technology (IT) networks, data centers, the cloud, mobile platforms, and other assets. Individual agencies rely on this cyber infrastructure to perform almost every mission-critical function within their purview, from national defense and natural disaster response to postal services and the constitutionally mandated census. In many cases, multiple agencies are interconnected at various operational levels to facilitate the sharing of business systems information and/or to provide interagency support to meet common mission objectives. The widespread adoption and use of cyber systems has immeasurably benefitted the country through increased government responsiveness, agency effectiveness, worker productivity, and a host of other economic efficiencies and returns.

Because we require cyber infrastructure to perform the modern-day functions of government, sophisticated and aggressive cyberattacks perpetrated by criminal entities and foreign government agencies represent a clear and persistent national security threat to the U.S. Government. As you know, there have been well-publicized cyberattacks, including the Office of Personnel Management (OPM) breach, which compromised the personal data and security of over 21 million current and former federal employees.

We are also experiencing an unprecedented level of cyberattacks in the private sector. As an example, in recent weeks the well-publicized security breach of a large credit reporting agency creates the potential that the personal data of well over a hundred million of United States citizens has been potentially compromised. This summer several ransomware attacks including WannaCry crippled the operations of a major global shipping company, one of the largest package delivery companies, a major drug manufacturer, as well as several healthcare providers. The reality is that global technology companies, like VMware, in cooperation with our customers observe a constantly growing increase both in incidence and sophistication of cyberattack – both from and upon systems inside the U.S. and overseas.

Internet of Things (IoT) Security

The emergence of the Internet of Things (IoT) is a technological step in which more and more aspects of the physical world, from manufacturing to banking to home monitoring to healthcare, transportation and even "smart cities" are interconnected and coupled with analytics and intelligence. The insights gained drive increased performance and efficiency of our infrastructure and bring new services to almost every aspect of our daily lives. Some consider IoT to be "the next Industrial Revolution." Unlike most traditional computing devices, many of these IoT Things will be directly connected to important physical aspects of our lives – from smart meters to factory robots, from cars to traffic lights, and even to devices in our own bodies such as insulin pumps and pacemakers. We will see a significant increase in IoT Gateway devices that aggregate and manage large collections of IoT devices in close proximity to the IoT device. These IoT Gateway devices are often powerful with some datacenter-like characteristics but will be deployed well outside the safety of traditional physical datacenter boundaries – in cars, on oil rigs, as part of the power grid, in factories, on cell towers. Indeed, several recent studies, including a recent Business Insider survey, estimate, "There will be 34 billion devices connected to the internet by 2020, up from 10 billion in 2015. IoT devices will account for 24 billion, while traditional computing devices (i.e. smartphones, tablets, smartwatches, etc.) will comprise 10 billion."

This level of interconnect will lead to exciting new capabilities in our ability to manage and optimize the infrastructures of our country, from manufacturing, to transportation systems, water management systems and many others – but also makes it critical that we secure the IoT from those with malicious intentions.

- It is vital, that we secure IoT infrastructure to prevent the compromise or disruption of our economy. This infrastructure, which among other things, will now form the basis of how factories and cities critical infrastructure interfaces with the real world.

- Securing these devices before they can be used as entry points or vectors to attack other parts of cyber infrastructure is paramount to overall strong cyber security.

The threat and impact of IoT based cyberattack is not theoretical; it is real. We have seen the impact and vulnerabilities from last year's distributed denial-of-service (DDoS) attack targeting outdated devices that did not correctly utilize the industry's standard best practices for cybersecurity. That attack took down major internet platforms and disrupted internet services for millions of Americans. The major wave of ransomware attacks this summer that wreaked havoc in the industrial, healthcare and logistics sectors were enabled in part by vulnerable devices that were not built securely or with patching in mind.

Importance of Cyber Hygiene

While there is certainly no silver bullet or single solution to prevent cyber-breaches generally or within IoT specifically, we believe that many of major breaches in the last few years would have been dramatically reduced or entirely eliminated if some fundamental principles of cyber hygiene had been followed. We propose five core cyber hygiene principles (below) as a universal baseline: the most important and basic things that organizations and the federal government should be doing. The concepts are not new but are key in moving to more effective security. They are rooted in well-established frameworks such as the NIST Cybersecurity Framework (CSF) and are technology-neutral.

1. Least Privilege	If a least-privilege environment has not been effectively implemented and users are provided with higher levels of access than they need, attackers can steal these users' credentials (user name and password) and gain broad access to systems. For example, it is understood, in the Target and Sony breaches, attackers were easily able to gain administrative-level privileges.
2. Micro-segmentation	If micro-segmentation has not been effectively implemented, attackers can break into one part of the network and then easily move around to other parts. For example, it is understood, in the Target breach, after an initial intrusion into the HVAC system, the attackers were able to move around to the payment network system. In the Sony breach, the attackers were also able to move around from one part of the network to another. In the case of the OPM breach, the attackers obtained access to OPM's local area network and then pivoted to the Interior Department's data center.
3. Encryption	If encryption has not been effectively implemented, attackers can exfiltrate data in readable form. For example, it is understood, after a data breach at Royal & Sun Alliance Insurance PLC, government investigators determined that the company had not adequately encrypted the data.
4. Multi-Factor Authentication	If multi-factor authentication (MFA) is not effectively implemented, attackers can obtain passwords and use them to access systems. For example, it is understood, in the OPM breach, if the contractor log-ons had been enforced with a risk-appropriate level of MFA, it would have limited the ability of the attackers to use the stolen credentials of the government contractor. In the case of the breach at LinkedIn, the hack exposed inadequately protected passwords of 100 million users. Since consumers often use passwords on

	multiple sites, MFA would have reduced the risk.
5. Patching	If patching is not effectively implemented, attackers can exploit open holes in systems. For example, it is understood, the ransomware attacks such as WannaCry exploited known software vulnerabilities for which patches were available. Organizations that fell victim had failed to effectively patch.

With education firmly in place, these five pillars of cyber hygiene are key in moving to more effective security.

VMware's Vision on IoT

Because VMware is the leader in datacenter and IT infrastructure management, we have a unique perspective on ways to secure the IoT ecosystem. With the advent of the Internet of Things, as more and more connected things are added to your network, it is a natural evolution of VMware's capabilities to now go out to the edge and help IT manage this new infrastructure.

Consumers, businesses and government need to feel confident that IoT technologies are secure and their information is protected. At VMware, we have advanced IoT products and software applications that embed each of the five cyber hygiene principles laid out earlier.

A way to secure the IoT ecosystem is by ensuring flexible and isolated connection points through secure manageable infrastructure, such as IoT Gateways. Whenever an IoT device connects to the internet, whether by itself or through an IoT Gateway, that system needs to be manageable, deployed responsibly with a proper initial configuration, and maintained at the current state of best-security-practices available throughout the complete lifetime of the device.

IoT Gateways are an integral part of the IoT infrastructure. They bridge, but also decouple, the physical IoT devices from management components in data centers. This bridge allows data and control to move securely from the device to the cloud or data center. We need secure IoT Gateways to ensure data and information are secured as it moves through the IoT pipeline.

The Internet of Things (IoT) Cybersecurity Improvement Act of 2017

As Congress and the Administration continue to work on policies promoting the IoT economy, we believe that it is important to seek input from industry stakeholders. Security needs to be paramount to protect sensitive data and information, as well as securing critical infrastructure. We believe it makes sense for NIST and other relevant federal agencies to cooperate with industry stakeholders in order to develop a set of standards and principles for IoT security. This is equally, if not more important, when federal agencies purchase IoT devices.

VMware applauds Senators Warner (D-VA) and Gardner (R-CO) for their bipartisan leadership in crafting the Internet of Things (IoT) Cybersecurity Improvement Act of 2017. We believe that the proposal is innovative when it comes to IoT security. We also commend the Committee leadership for releasing a Discussion Draft of the Senate proposal to seek additional stakeholder input.

There are several provisions of the proposal that VMware specifically supports. For example, we believe IoT devices should, from the outset, be designed with vulnerability patching capabilities built-in. A simple patching requirement could have drastically reduced or eliminated the WannaCry and similar ransomware attacks. In addition to the patching requirement, we support several of the cyber hygiene concepts in the proposal, which include micro-segmentation and multi-factor authentication. The concept of micro-segmentation would play a critical role in ensuring that IoT related data and information are segmented and properly protected against IoT cyberattacks. This would go a long way in providing additional layers of security to protect sensitive data and information in the IoT ecosystem. We also support the security considerations included in the proposal that would be provided by IoT gateways. If an IoT device lacks a minimum level of patching security, requiring systems like IoT Gateways would provide an appropriate layer of security protection for consumers, businesses and the federal government. IoT Gateways are embedded with many of the core cyber hygiene principles such as least privilege, micro-segmentation, patching, multi-factor authentication and encryption.

In all, the **Internet of Things (IoT) Cybersecurity Improvement Act of 2017** is an important, bipartisan step forward in promoting a secure federal IoT ecosystem.

Summary

The global digital ecosystem is experiencing an unprecedented level of sophisticated cyberattacks. In order to secure and adequately protect our customers, products, services, and networks against these highly sophisticated attacks, we must utilize every security tool we have in the toolbox. The IoT economy presents a significant opportunity for U.S. companies. Billions of IoT-connected devices will be on the free market for consumers, businesses, and government to consider purchasing. The U.S. has a ripe opportunity to claim global leadership in the IoT space. The IoT economy will create American jobs and could be an opportunity to boost American manufacturing across the country.

The IoT economy will also provide new efficiencies for consumers, schools, hospitals, and manufacturing, as well as federal, state and local governments. Security is the key principle that will enable and advance further adoption of IoT. If consumers, businesses and government do not feel that IoT products are secure, it will only hinder U.S. global leadership in an inevitably growing and innovative IoT economy.

Promoting good cyber hygiene should also be a key goal that helps agencies, consumers and businesses better protect their information and networks from malicious attackers. One of the best ways for the Federal Government to be proactive is by deploying micro-segmentation technologies that offer the ability to segment their networks in the event of a breach.

The **Internet of Things (IoT) Cybersecurity Improvement Act of 2017** provides a thoughtful framework, modeled after the industry-recognized NIST framework, for the federal government to put forth some baseline security recommendations to consider when specifically purchasing IoT-related and edge-computing devices. We are pleased that the proposal includes important cyber hygiene concepts, such as patching, micro-segmentation and multi-factor authentication. We also support the considerations included in the proposal that leverage the security benefits introduced by properly managed IoT gateways, which can act as isolation and management gateways to help prevent and remediate any comprise of connected devices. VMware commends Senator Warner and Senator Gardner for introducing this legislation, and we applaud the efforts of the Committee for putting forth the discussion draft for additional stakeholder input.

I appreciate the opportunity to share my thoughts on this very important issue. We applaud the leadership and vision of Chairman Hurd and Ranking Member Kelly for holding this hearing. VMware looks forward to continuing to work with the Committee on this and other important issues. Thank you again for the opportunity.

Mr. HURD. Thank you, Mr. O'Farrell.

Now, it's with great pleasure to recognize the gentleman from California, Mr. Darrell Issa, for his first round of questions.

Mr. ISSA. Thank you, Mr. Chairman.

And I think the public, in hearing we're doing something on the Internet of Things, probably in spite of your testimony would consider that, well, this must be new. But, Mr. O'Farrell, I'm going to use you and a little bit of our gray hairs to establish something for a moment.

When you began in the industry, people were dialing, auto dialing to find modems and then trying to invade people's systems that were connected by modems, correct?

Mr. O'FARRELL. That's correct, yes.

Mr. ISSA. And the advent of firewalls and private systems, VPNs, point-to-point connection was in response to that and other challenges, right?

Mr. O'FARRELL. Yes. Broadly bringing a level of security and protection.

Mr. ISSA. So is it fair to say that the products that the public is hearing today, the Internet of Things products, could be set aside in totality and we could have this discussion today only about connected—externally connected computers, whether mainframe minis, if they were still around, or micros?

Mr. O'FARRELL. So there are similarities in the existing data center infrastructure, and, in fact, you would see many of the same issues appearing, how do I secure my infrastructure, how do I protect it, feeding back out into the world of IoT. I think there is one difference, though, to highlight, and the difference is, unlike your typical data center infrastructure, you are not protecting just data; obviously, that's important to protect, but you're protecting physical infrastructure. These devices can be controlling equipment in a hospital.

Mr. ISSA. Sure.

Mr. O'FARRELL. So there's different aspects.

Mr. ISSA. But if you're controlling the electric grid, you're controlling thousands of hospitals, right?

Mr. O'FARRELL. Correct, yes.

Mr. ISSA. So using that as a reference, would you all agree, if you can, that, in fact, this is not a new problem, but what we're really dealing with is a problem that goes back to the first connected product that had access even by telephone to the outside? That's fair to say, right?

Okay. I'll take no noes as a yes for now. But let me follow up by asking you all a question. When we look at a fully qualified domain name, in the IPv4 world, our problem was we ran out of numbers to distinctly connect points so we could identify a point and its effective location. Is that a fair statement, for those that have been around? And then we went to IPv6 in order to have enough points that we could identify uniquely. Anyone? Mr. O'Farrell?

Mr. O'FARRELL. Yes, IPv6 increases the number of available addresses enormously.

Mr. ISSA. So as we're here looking at the question of a lot of things that are going to be done, would it be fair to say that the ultimate solution for point-to-point connections and conversations is, in fact, to eventually have every point in some way be fully qualified and fully identified so that when the chairman has a product that's being addressed by a product asking it to do something, its chances of it being anything other than an approved product reasonably asking for that information can be dramatically reduced? In other words, you can no longer spoof the way the bots do, spoof an event to get somebody to do something that they wouldn't do if they knew who you were? Is that a long but fairly accurate statement?

Mr. CORMAN. Such a maneuver would help certain aspects of the threat model, but not all. And to also respond to your prior point, while things like the NIST cybersecurity framework and things like remotely exploitable modems are familiar and we can glean from the past, there are material differences. The Cavalry has published a framework of six differences, which are at least good questions to marshal yourself through, and succinctly they are—they're different adversaries with different motivations. They're different consequences of failure, including public safety human life. Different environmental contexts where you're not going to have layered defenses. Different composition of goods. Different economic realities for margins and costs to goods, and different time scales for time delays.

Mr. ISSA. You know, I appreciate all of that, but that's sort of like saying that the horse and buggy has nothing in common with the car when you're just trying to get to church. The reality is that—the reason I asked this line of questioning with my limited 5 minutes is, what it appears to this member, who has been around since the 1970s as a manager of a computer facility in the military, is we have old problems that have never been resolved. We now are in a position where quicker, faster, and with greater devastation the problems can lead to catastrophic problems for our society, for human life, and yet in a sense we've never resolved that great question, which started off with the modem that said you can call me, but I'm only going to call back to the number that's programmed in me, that two-way authentication that came out back in the modem day.

In a sense, the reason I ask the question, and I'll close, Mr. Chairman, is it appears as though unique and thorough, fully qualified identity with the appropriate authentications is going to have to be part of any solution or you're going to have exactly what happened to Jared Kushner's lawyer who emailed "forward" to a spoofer what he was supposed to send to the son-in-law of the vice president only a few days ago, because you've got to know who you're talking to or, inevitably, all the security in the world won't do you any good when you send it to the wrong place.

Mr. Chairman, I'll take that as a yes if they don't revise and extend on it, but it's an area of concern, and thank you for continuing this.

Mr. EGGERS. You know, if I may, let me just throw in a couple of thoughts that, A, we share your concerns about security and making sure that as we go from, let's say, device to end user, as we expand and we want to the Internet of Things, we're doing it in a way that minimizes those risks. Authentication is a key topic. I know we at the Chamber, we have supported the TENS stick, the trusted authentication concept and effort that was launched in 2011.

But I think to your bigger point, we do share your concerns about security and the need for increased security and risk management. One thing I think we would look to is some kind of a layered approach, right? No single one thing is going to get us to where we want to be. And I would also want to look closely at what kind of measure metric we look to get there. We at least in—at the Chamber, there are private sector-led efforts to look at whether or not a device, widget, gadget is more secure, let's say, than another. We probably would be a little skeptical or at least want to proceed with caution if government's going to put a thumb on the scale. It may be premature to at least select one certification model versus another.

I'll finish there. Thanks.

Mr. HURD. Ranking Member Kelly is now recognized for her opening questions.

Ms. KELLY. Thank you.

As the IoT market continues to grow rapidly, there are concerns that it has grown without proper security standards or market incentives to safeguard against bad actors. We haven't done a good job of rewarding good actors who bake in security. But for the Federal Government uses, an unsecured device poses a great threat to information security and sensitive data.

A 2017 report by the Government Accountability Office found that IoT device vulnerabilities can be caused by, and I quote, "a lack of security standards addressing unique IoT needs."

Mr. O'Farrell, would you agree that IoT devices pose a unique cybersecurity challenge?

Mr. O'FARRELL. Yes, I would. Partially because the impact of a cybersecurity breach on an IoT device, as we've noted, can affect something very real in the physical world, including human life.

Second of all, IoT devices by their nature are not behind a brick wall in a data center. They're at the bottom of oil wells. They're in factories. They're in buildings, which means the ability to physically attack them or interface with them becomes possible. Therefore, I think that a layered approach as to how you secure it becomes more important.

So the bill mentions, for instance, use of IoT gateways and microsegmentation. These are second order of protection, which can be used to protect those devices themselves, even if they become compromised in some way.

Ms. KELLY. And so you agree that establishing at least minimal cybersecurity standards would help prevent IoT device vulnerabilities?

Mr. O'FARRELL. Yes. I think in the context of the bill, which is essentially highlighting the existing NIST standards from a cybersecurity point of view and applying them to IoT in the context of the Federal Government procuring those devices, yes, I do.

Ms. KELLY. And, Mr. Corman, would you agree?

Mr. CORMAN. I do. And there's several things we could do. We wanted to focus on things that were 80/20 rule-ish. And I think if you squint—everything really hovers around vulnerabilities that are known. Known vulnerabilities are more than 30 percent more likely to be attacked by adversaries than unknown. And we discussed this with Chairman Hurd in Las Vegas. We had this notion of IoT really should have five postures towards any failure. They're going fail. They're going to fail often. How do you avoid failure? By building security in versus building on. How do you take help avoiding failure? From willing allies like through coordinated disclosure. How do you capture, study, and learn from failure? With logging in evidence. How do you respond to failure? With security updates and patching. And how do you contain and isolate failure? With segmentation and isolation to fail safely.

And those are really you must be this tall to ride the Internet of Things kind of concepts. Obviously, there's so much more we could do, but that's a really minimum viable—I once said unpatchable IoT are the lawn darts of the internet in that they are inherently unsafe.

Ms. KELLY. Thank you.

Both the House and Senate versions of the IoT Cybersecurity Improvement Act require minimum security requirements from vendors selling IoT devices to the government. These include basic best practices like federally procured devices being patchable and not using hard-coded passwords.

Mr. O'Farrell, do you believe these standards are reasonable?

Mr. O'FARRELL. Yes, I do. I also note that the bill gives, under some circumstances, the ability to be able to waive those if a device does not support that, as long as another security technique is put in place.

Ms. KELLY. Right. And can you describe how these practices, basic hygiene, can provide a reasonable level of security for the government to feel confident in purchasing IoT technologies?

Mr. O'FARRELL. So you've already heard to some degree how IoT, sort of the existing ways that you secure data centers and infrastructure, also applies and becomes applicable in some way to IoT. Many of the things which are described here, authentication, microsegmentation, least privilege access, all of those are core concepts described by NIST to secure data center infrastructure and cyber infrastructure, so the same would apply equally to IoT.

Ms. KELLY. Thank you.

Mr. O'FARRELL. It just becomes an extension—I'm sorry. It just becomes an extension, essentially, of the existing data center infrastructure.

Ms. KELLY. Okay. IoT devices promise exciting opportunities and benefits we cannot ignore, as all of you agree the security implications. Government data must be protected, and it is essential that we address the cybersecurity concerns now rather than retroactively. The IoT Cybersecurity Improvement Act provides basic security standards that are necessary for protecting government data and can set a positive example for the IoT industry at large. I believe the legislation serves as an excellent starting point for IoT security. And I yield back.

Mr. HURD. I'd like to thank the ranking member.

And if my memory is correct, Mr. Gianforte, this is your first—this is your first hearing with us. It's great to have someone with your background, experience, and patents on this committee. And you're now recognized for your opening 5 minutes of question.

Mr. GIANFORTE. Thank you, Chairman Hurd and Ranking Member Kelly. It's my pleasure to be here. Thank you for the testimony that you're providing for us today. I appreciate the effort. We need to make sure that our government is secure, and particularly the Internet of Things security is important.

I want to ask questions in two areas. And as Chairman Hurd mentioned, I ran a cloud computing business for many years, and we had thousands of clients. We had over a thousand cyber attacks per day that we had to defend against, so I have some familiarity here.

I'd like to talk a little bit about NIST vulnerabilities. How often does NIST publish updates on vulnerabilities? Just based on your knowledge, Mr. O'Farrell.

Mr. O'FARRELL. I don't actually know the exact number. I know we get vulnerabilities from NIST, but also from broadly across the industry. You know, large software companies like Microsoft and others would publish those vulnerabilities as well, and so it would not be unusual to see a steady stream of vulnerabilities coming in every month.

Mr. GIANFORTE. Every month there would be new ones?

Mr. CORMAN. Every day.

Mr. GIANFORTE. Every day there's updates.

So are all vulnerabilities, Mr. O'Farrell, created equal or are some more severe than others?

Mr. O'FARRELL. Some are more severe than others. The challenge with the vulnerabilities, you can't always tell or predict whether the vulnerability is going to be exploited in some way. Remember, a vulnerability simply says there is something here which could be a problem. It doesn't say this has been used to attack or exploit in some way. So you have to be careful with respect to how you rate vulnerabilities, but there is a rating for vulnerabilities and they are not all created equal.

Mr. CORMAN. If I may add to that, we have a common vulnerability scoring system for various factors. We have recently learned it's insufficient for safety critical, and there's a special project through MICR to look at safety critical in hospitals, for example.

Mr. GIANFORTE. But to your point earlier, Mr. Corman, some are more important than others from a risk perspective.

Mr. CORMAN. Well, for consequence severity and context, yes, but there's also one more thing in the written testimony I'd like to call out, which is that for all known vulnerabilities there are a special subset that if they're in created attack tools or if they're in an exploited database, they're 30 times more likely. So your heavier risk-based clustering of this to enhance the yield.

Mr. GIANFORTE. Mr. O'Farrell, where I'm driving here is, in a complex system that includes an operating system, maybe an application server, an application communication software, all of these systems are collections of various components. Given the frequency with which vulnerabilities are published, is it possible for a complex system to have no vulnerabilities over a 12-month period?

Mr. O'FARRELL. I think it is highly unlikely. I think that, in fact, you have to expect and to some degree that there's probably some vulnerability in there. It's complex. It's got many pieces of software and products. And I think if at all possible, you need to build into your security stance the expectation that you're going to have to adopt and deal with some form of exploit should it occur. So control and second-layer protection is a part of the story.

Mr. EGGERS. Sir, if I could—go ahead, sir.

Mr. GIANFORTE. And I raise this, because in the legislation as it stands today it says that all procurement by the Federal Government will have no vulnerabilities. And I just want to highlight that some are more important than others. We may want to differentiate in some way.

Mr. EGGERS. I think—I was just going to add that I think that a focus on, A, a definition of what we mean by "internet-connected device" I think is crucial. B, I would say that you are right, NIST, its database of vulnerabilities ranks low to high. US–CERT pushes out vulnerability and other update information, if you will, regularly. I get them.

One of the things I think that's relevant, at least in terms of the conversation here, is I think everybody is right to focus on the vulnerabilities and to upgrade fix. One of the issues, at least in terms of if you are a provider, and one of the questions that we've got is there's a requirement for tracking notification.

Mr. GIANFORTE. Mr. Eggers, if I could just claim my time back.

Mr. EGGERS. You may, sir. Of course.

Mr. GIANFORTE. Thank you.

And I just wanted to, in my remaining 50 seconds, Mr. Ross, I have a question about standard practices in the software industry. As in the legislation there are particular clauses that require manufacturers of Internet of Things to provide perpetual updates to software, and I think the process of providing a way to do update is good. In the software industry, is it standard practice that that's done as part of the initial purchase price of the product or is there typically a separate maintenance contract that is designated to ensure that you get updates to your products?

Mr. ROSS. I think that very much depends on the product. You know, so you see, obviously, we all have apps on our iPhones that get free updates, you know, without paying any extra, and other companies provide update services as a separate package.

Mr. GIANFORTE. And if there was a requirement to provide perpetual updates, what impact would that have on the initial purchase price of the product itself?

Mr. ROSS. Again, I think it depends on the business and its sort of, you know, business model how it generates revenue, so I don't think there's a single answer for the entire——

Mr. GIANFORTE. But if a vendor had to provide more services, typically prices would go up?

Mr. ROSS. You could certainly expect that in some cases.

Mr. GIANFORTE. Okay. Thank you.

And I yield back. Thank you for your patience, Mr. Chairman.

Mr. HURD. Thank you.

Mr. Raskin, you're now recognized for 5 minutes.

Mr. RASKIN. And thank you very much, Mr. Chairman.

So I'm interested in last year's cyber attack with the Mirai botnet, which took down the internet for most of the East Coast. And it was an attack that preyed on the Internet of Things connected devices like web cams and routers and so on. And as I understand it, it infected the IoT devices with malware, and then the hackers were able to gain control of the devices and use them to drive an overwhelming amount of traffic towards the target.

Mr. O'Farrell, let me ask you, in the aftermath of the Mirai botnet attack, it was revealed that the attackers had used only about 20 percent of the computing power of 20 percent of the entire botnet, so in other words, a small fraction of a small fraction of the actual capabilities. How would a similar attack ramped up affect the Federal Government, if they came after us?

Mr. O'FARRELL. I think the ramp-up would have an equivalent ramp-up in terms of impact. Now, obviously, after that attack, organizations will have looked at other ways they can protect from such a denial-of-service attack, so it would have been some changes made to try and protect against that. But if the full force of that attack had been used at that time, with the internet as it stood at that time, it is likely the impact would have equally been proportionally large. So in terms of the Federal Government, it would have brought down major internet providers, and that in turn would have begun to affect what the Federal Government does day to day.

Mr. RASKIN. Gotcha. Many of the IoT devices are shipped with hard-coded passwords that are unable to be patched or updated. What risk does a hard-coded password or device present to our ability to respond?

Mr. O'FARRELL. So I think as Congressman Issa mentioned, you can identify these devices in terms of an IP address of some sort, whether it's IP6 of or IP4, however, the actual identification of the device in terms of—sorry, of somebody accessing the device is typically handled by a password of some sort.

A hard-coded password is typically very early somebody posts that on the network. You'll get a message on the internet saying if you're accessing this camera, these types of camera, here's the type of hard-coded password. So effectively you have no password, which effectively means then those devices are open for people to access them and then try and exploit them in some way.

Mr. RASKIN. Thank you much.

Mr. Corman, how does Senator Warner's bill address that issue? Are there other legislative measures that we should be contemplating to deal with that problem?

Mr. CORMAN. One of the things I wrote in my written statement just in full disclosure is that Federal procurement alone won't stop the next Mirai botnet. The government does not buy enough of those devices, and the overwhelming majority of the ones that hit the internet that afternoon were from Vietnam, outside the country purchased by others.

What we like about the bill is the fact that it sets, by example through purchasing power, a model that can be replicated by hospitals, other organizations, and the international policy community in a reasonable way. There are some very ugly and dangerous counterproposals, such as bricking devices; doing deep packet and inspection at the carrier, the edge, which could get into net neutrality issues; and balkanization and Geo-IP filtering that would play directly into the hands of Russia, China, and some of the people who tried to take over the free open internet a few years ago and nearly succeeded. So there are other things that can be done, some of them having very dangerous side effects for the economy and for U.S. interests.

Mr. RASKIN. Let me just follow up on that. The use of these IoT devices is expanding rapidly around the world. I think it's estimated that by 2020, there could be more than 20 billion of them. Does that increase our exposure? Does it make it a more dangerous situation?

Mr. CORMAN. Yes. I used to be the director of security intelligence for Akamai, which handles the largest denial-of-service attacks in the world, and the math doesn't handle even Mirai. It certainly won't handle the growth rates.

So while I really like some of the hygiene principles to lead by example, these have to be adopted by the private sector, whether through self-regulatory, through purchasing, through free market forces. But this bill alone won't stop the next Mirai, but it sets an example that could make more devices higher hygiene than lower hygiene.

Mr. RASKIN. Do you—and I could open this up, does the panel think that manufacturers are doing enough to ensure the security and the safety of the IoT devices?

Mr. CORMAN. No.

Mr. ROSS. So I think some are and some aren't. And I think, you know, what we need to do is incentivize those who are, you know, providing good security and building it into their products to have more opportunities, including through government contracting, and to have that good work recognized. And then we need to find ways to incentivize those who are not doing a good enough job to do better. So I think they're not all the same, but certainly there are some actors out there who are not taking security seriously enough.

Mr. O'FARRELL. I mean, I think I would echo the sense that, one, they're not all the same, but, two, for those who do do the good job, you know, to make sure that they have the benefit of being able to, you know, fit the requirement policies of the Federal Government. That's a positive message to them, and it's rewarding the people who do the good job as opposed to those who do not.

Mr. EGGERS. If I may, I think the intent of the bill to bring more secure devices into the Federal Government is sound. Very sound. It is how we get there, I think, that's the trick.

In terms of working with so many different businesses across multiple sectors, I think Tommy's right. We're kind of in a gray zone where I think, if anything, when I step back and I look at a bill like this, I say, how can we make sure that the companies that are making devices securely—and there's a lot of standards out there. There are a lot of companies building devices according to this or that standard, guidance, or best practice. I want to make sure that they're the ones that win and, ultimately, consumers, the purchasers, will too.

Mr. RASKIN. Thank you. I yield back, Mr. Chairman.

Mr. HURD. Thank you.

Mr. Mitchell, you're now recognized for 5 minutes.

Mr. MITCHELL. Thank you, Mr. Chairman.

Let me ask the panel, whoever wants to jump in on this question, you talk about government standards and those standards generating more confidence in the private sector as well. How much confidence do you have that, in fact, government-mandated standards are going to improve the circumstances?

Mr. CORMAN. One of the things I like here is it's not the government mandating standards for the private sector, it's the government as a purchaser acting in their own selfish interests to protect the interests, not just against larger scale DDoS, but against the next OPM breach or against people surveilling your offices or any and other number of things where our smart TVs or smart gadgets could be a risk. So this is more leading by example than forcing something. It could catalyze innovation.

Mr. MITCHELL. Let's talk about—give me a second, and I want to hear from everybody else—leading by example to Federal Government. Last we had a hearing several weeks ago, maybe a couple months ago at this point, there were 143 chief information officers in the Federal Government; 143 of them was I think the count. How does that give us confidence? I mean, I ran a fair size private company. There was one CIO who I held directly accountable for our security of all things, not just our internet access, but all the other applications we used. I'm concerned that with 143, I'm not sure we're going to get anywhere near the level of concern we have. How do you feel that's going to help us?

Mr. CORMAN. I think we're getting the critical mass slowly. The Presidential Executive Order on cybersecurity, two quotes, The Federal Government "has for too long accepted antiquated and difficult-to-defend IT," and, "Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced."

The DHS' six strategic principles for IoT covers this. The Presidential Commission, FDA, Department of Transportation. There's a critical mass forming around what some of these are and an increased recognition that what we had been doing don't work across those federated CISOs to treat the Federal Government as an enterprise.

Mr. MITCHELL. Okay. Mr. Eggers?

Mr. EGGERS. Congressman Mitchell, if I may, to your point about standards, I think standards are really important. Our companies live and breathe by standards. They are successful because they use standards that are private sector led, industry driven, global in nature very often.

The thing about the bill—again, the intent about bringing secure devices into the government is sound. I think one of the things we want to look at is are we scoping the device of the definition of internet-connected device adequately? And I think the answer is we don't know really yet. I think one of the things we'd like to do is talk with groups like NIST, NTIA to help inform how we make that decision. It's very broad. It could capture low-end devices that really aren't intended to be plugged into the bill. It does consider, obviously, devices that are at least capable, but should they? It's not clear. In many cases, they shouldn't be.

One of the issues I will—and then I'll finish, is one of the issues about tracking vulnerabilities and making patches and upgrades is you could find a situation if you're a contractor—and that term too is vague—the lengths at which they've got to go to track virtually any known vulnerability, and there are a lot of avenues for finding those, and you would be beholden to quite a notification structure, and so that gives me pause. The idea about upgrading is sound, but the notification, among other things, gives me pause.

Mr. MITCHELL. Mr. O'Farrell, you had a comment?

Mr. O'FARRELL. Maybe two things. One of them, in terms of the—you know, as a taxpayer looking at the Federal Government purchasing IoT infrastructure, I would like to know that they're getting value for their money, and security is a key part of that.

Mr. MITCHELL. Absolutely.

Mr. O'FARRELL. So that's where I see those key guidelines. They represent what is a reasonable model around security.

With respect to the broadness of the definition of IoT, yes, I think devices at the edge, they're difficult to describe, and they'll probably see opportunity to focus a little bit more on describing that, but the legislation does describe mechanisms that says, if devices are simple enough such that they cannot meet all of the requirements with respect to patching and so on, that there are some waivers associated with that.

With respect to describing vulnerabilities, I think the bill specifically is trying to imply you should not be delivering equipment with known vulnerabilities, and then based on patching you get to fix those vulnerabilities, if and when they appear and when you find out about them. That's why the patching is a critical part of the story when combined with recognizing that vulnerabilities will occur.

Mr. MITCHELL. Mr. Ross, you had a comment. The last few seconds here.

Mr. ROSS. Sure. I will try to make it quick. But I think, you know, as you look at the Internet of Things, it really does describe a really broad array of devices, including, you know, at one end, sensors that don't even have operating systems and are designed to be cheap and mass-produced and can be so, while minimizing security risks, depending on how they're deployed in a network environment.

And at the other end, you know, looking at, really, life-critical systems, as Mr. Corman has discussed. And I think that definition, it's really important that we capture it, because there is a cost-benefit equation here. And in some cases, the government is going to want to be able to buy devices that are inexpensive and mass-produced without having to build in a lot of security features that would drive up the cost and make them unsustainable. And you think about things like sensors and infrastructure that you want to put in place and leave for 50 years just to tell you, you know, seismic activity over time.

I think that security standards are very important, but being calibrated against risk is what allows us to drive security in the most sort of efficient and rational way.

Mr. MITCHELL. One other quick comment and I'll yield back, Mr. Chair, is that you mentioned incentivizing them, and in my mind, it's also creating systems that the general public understands what the government is doing so they can assess how they do that. And today's hearings raise concerns for me. I have a camera system in my house for security, and to be absolutely blunt with you, it's a small town, and I can access it on my phone, I'm not sure if it has patches and what they do to patch it. I should know better.

So I'll yield back.

Mr. HURD. Mr. Corman, did you have a——

Mr. CORMAN. Yeah, I'll be very brief. Some of Representative Gianforte's comments, and your own, they kind of make the case for what I said earlier about the value of software bill of materials. If it is unrealistic to perpetually update,if it might cost more money, if the company has gone out of business—the camera manufacturer—these things allow at least the procurer to assess, am I affected, where am I affected, should I unplug it? And there are a series of use cases that this would ameliorate or soften with that increased transparency.

Just like a bill of materials or food label, like if you're allergic to peanuts or if you're allergic to some sort of food and, you know, having some sort of ingredients list allows me to make a choice. And if there were a recall, if we did find out there was a bad batch of a certain ingredient in the food we ate, we know to stop eating it. And such a function could be applied to IoT and software as well.

Mr. MITCHELL. Thank you, Mr. Chair.

Mr. HURD. Thank you.

Now I recognize myself, and not necessarily for as much time as I may consume, but I'm going to take my time.

Mr. Ross, maybe we pick up on a comment you just made. If a censor doesn't have an operating system, how can it be used in a DDoS attack?

Mr. ROSS. So, again, it really depends on—and I think one of the things that we need to think about when we're thinking about IoT security more broadly is not just how a device functions, but how a device fits into a broader network. And, you know, Mr. Eggers has mentioned taking a multilayered approach. How we build in security at different levels within a network can really shape outcomes far beyond the individual device. That said——

Mr. HURD. But should the person developing that censor take those concerns into, as they're developing, how that censor works?

Mr. ROSS. I think the person developing the censor needs to be able to respond to the demand for the product, and security ought to be part of that demand. But you can imagine a situation in which you might want to deploy, for example, a lot of sensors with limited security built into the devices themselves but adopting network solutions that allow you to manage security through cloud services, through network security mechanisms that use those devices in a controlled way,and even patch them through cloud-based services rather than patching individual devices.

You know, the innovation around security approaches to securing IoT devices and other devices is incredible. And really, you know, we're seeing innovation in the security space keep pace with innovation in the product space. In other words, there's new approaches to security that we're seeing every day. And so I think it's really important, as we craft policy, not to limit the ability for those network-based solutions to sort of take hold.

Mr. HURD. And I'll ask this question again to you, Mr. Ross. And then, Mr. O'Farrell, I'd welcome your thoughts on this as the software guys here.

How difficult is the code to have—to update a widget or a device that we're considering part of the Internet of Things? How difficult is that code to write? Is that standard code? Is it something that is open source information out—open sourced out there where you pull that module and say, hey, here's how we do it? Is there a commonly accepted way of doing that?

Your thoughts on that. Mr. Ross first, and then Mr. O'Farrell, your opinions.

Mr. ROSS. Sure. The two gentleman to my left probably have a better technical background to answer that, but I would say, you know, 2016 IoT developers survey found about 25 percent of IoT devices don't have operating systems. So accepting patches and that kind of thing is—you know, without an operating system is much more challenging.

That said, you know, I think the complexity of the codes sort of depends on the code base and the product itself and, you know, individual manufacturer's approach to coding. But I would defer to my more technically savvy colleagues.

Mr. HURD. I'll let Mr. O'Farrell and Mr. Corman and Mr. Eggers, if you have comments, I'd welcome that on this question too.

Mr. O'Farrell?

Mr. O'FARRELL. So in terms of broader applicability of patching, your PC at home is constantly patched. Every cell phone that's out there, from evenmajor manufacturers, is constantly patched. The applications living on those are constantly patched. So the concept of being able to say, is patching a well-known function, yes, it is.

I think where the challenge that Mr. Ross is pointing out, you may have a class of devices who are so simple that they don't necessarily have the ability to handle a software upgrade. They may not even have software at all. They might be a very simple device just relaying temperature or something. Under those circumstances, then you need to apply other techniques. You either need to have that device talk to a gateway, and then the gateway itself is patched and secured, or you do things with network segmentation or other network management capabilities to be able to secure that piece of infrastructure.

Mr. CORMAN. Just to add to that, some of it's knowing how to do secure updates over the air without making that a security risk itself. And we do know how to do that. That information is available. Some of it is going to raise the cost of goods on some of these devices because they need to future-proof a larger image than they started with. There are some IoT platforms that anticipate and build in the ability to do updates securely with encryption. There are some that are cheap, maybe too cheap to be safely used. So it's not a zero cost, but we know how to do it. Technically, there are platforms that could do it, and if we reward those that do.

And then lastly, the NTIA process for upgradability did say it could be an out of station based model, where you say, I am patchable, I commit to patching for X years. And that goes into the Federal Government's purchasing decision of, if I'm going to buy an unpatchable device, I'll have to spend more aftermarket, or just choose not to buy it.

Mr. HURD. Mr. Eggers, do you have an opinion?

Mr. EGGERS. Yes, sir. Quickly. So I was just going to add that I hear from members that much depends on the device and where it's supposed to be, with the kind of device, the operating environment in which it's supposed to function.

I think one of the challenges with protecting the Internet of Things is we are dealing with legacy devices that really weren't ever meant to be connected to the internet. And our colleagues will say, hey, then we build a security appliance, some kind of protective system firewall, what have you, around there.

So I think, at least in terms of engaging government, business to business, a lot of times they will work through these tough issues around software upgrading and so forth,what devices can do, what are their limitations. And I think that is really important to understand. There are certain devices that are meant to do some things and devices aren't supposed to do other things. And so I think our members, and generally what I hear is they're very cognizant about what devices can do and where they should go and how they should be protected.

Mr. HURD. So would it be fair—and I'll welcome all four of our illustrative panel's opinions on this. On this legislation when it says the IoT device must be patchable, would adding something to the effect of, if it has an operating system, and if not, then, X, Y, and Z?

Mr. CORMAN. I think the existing bill in the Senate anticipates this and allows for waivers and allows for NIST to specify compensating controls for devices that can't do this,as opposed to maybe making some brittle assumptions that may not hold up over time. I do like Ranking Member Kelly's comment about keeping some sort of advisory board to keep these vibrant and evergreen. I think a lot of the ones in the bill right now are evergreen, but we do want to make sure that this is—you know, there's no unintended consequences or byproducts of this.

Mr. EGGERS. I would say one of the items about the bill that I've noticed that seems to be helpful is it's forward-looking, right?We're trying to say, hey, let's project forward and say how can we do some things that we know we should do?

One of the issues that I think has come up with our members is the roll that third-party certifications may apply where that's applicable. We are in favor of private sector entities looking to different labels, certification models, if you will, but to have government possibly put a thumb on that scale seems to be premature——

Mr. HURD. Who is doing that right now?

Mr. EGGERS. Well, you've got different organizations. You've got UL. You've got different organizations providing, I think, approaches, let's say in Europe.

The challenge, I think, with this is the speed of the threat, the dynamic nature of trying to put, let's say contents, we're not clear about what contents would be in that label. Would it be proprietary information? What kinds of maybe software-related information would be on that label? Can it keep up with the threat? And then, at least in our experience, once kind of a selection by parts of government take hold, it's hard to extract ourselves from that model. Right?

Mr. HURD. So is there any scenario current or in the future that you can think of where you need to have a password hard coded into a device?

Mr. Eggers?

Mr. EGGERS. You know, I would say at least I've gotten positive feedback on the idea that once you receive a device, you should be able to change that pass code. That's helpful. But to your question, I'd have to get back to you.

Mr. HURD. So you've never had a member come to you and say, man, I really need to make sure that password is password in that device because it's not going to be able to function?

Mr. EGGERS. They would say that that is a bad idea uniformly.

Mr. HURD. Mr. Ross, do you have an opinion? I know there's like a bunch—we're on like three or four different kind of questions right now.

Mr. ROSS. Yeah, I know.

Mr. HURD. Throw it out there.

Mr. ROSS. Well, let me take your first question first on the patching. I think, you know, as you know, when product developers are considering how to approach a product, there's a few variables that are intentioned, you know. You have computing power, battery power, cost, size of the device. You add more computing power, you add more cost, you need more batteries, you increase size. So I think it's—I'm hesitant, when looking at the government's diverse needs for sensors and other IoT devices in a variety of different contexts, including national security, including infrastructure, I'm hesitant to say if you have an operating system, you need to be patched.

There are tradeoffs that you should make. And considering risk in, you know, how you apply security measures I think gets you a better outcome. It gets you——

Mr. HURD. So on——

Mr. ROSS. —security, you know, built to—calibrated to the risk that the devices pose.

Mr. HURD. So is there a scenario in which you would advise the Federal Government that operating some system that has an operating system to not patch that software?

Mr. ROSS. There may be. I mean, there are very small operating systems on very small devices, and we may have a need as a government. Again, you know, I come from——

Mr. HURD. Based on the level of threat or the vulnerability?

Mr. ROSS. Right. So I come from a national security background. And as you I'm sure know, the Department of Defense and the intelligence community, they want to put sensors on everything. And I've heard goofy proposals about putting sensors on cows to track their movements with pneumatic herders and see where those herders go. It happens.

The ability to deploy——

Mr. HURD. I may have been involved in a few of those conversations, by the way.

Mr. ROSS. Yeah. So, you know, the ability to deploy cheap mass-produced devices that may not pose a risk, a substantial risk to life, public safety, the economy and so on, may be a trade off that we want to be able to make for other purposes.

And I think, again, it's not to say that there shouldn't be standards;it's to say that the standards should be more nuanced than one size fits all, that there should be a risk framework that governs how standards are applied.

So back to your second question, I'm not sure that I can conjure up a scenario where a hard-coded password might be appropriate. The one thing I would say is that we have—you know, as you know, you're the champion of the modernizing government IT act that we desperately need. The government is using systems, and I'm sure I could read this off of the talking points around the legislation, that are 50 years old or older.That's true in a lot of different contexts. And many systems, you think about industrial control systems, are built to last a very long time. And what we're doing now is we're applying software and other devices retroactively to help manage those systems.

I know that we've heard from some of our members that managing those systems that are, you know, themselves very old and based on out-of-date protocols and that kind of thing, require solutions that may not be, you know, within the confines of the security standards on this bill.

That said, I don't have any specific use cases in which a hard-coded password would be necessary to the function of those kinds of devices.

Mr. EGGERS. And if I may, Mr. Chairman, come back to my answer about the need for, let's say, taking a device and changing the pass code so it's harder for a bad actor to commandeer that device. So I said uniformly it would be a bad idea. I think, generally speaking, most of our folks would say that's a bad idea.

I do wonder, because it has been raised, about, let's say, the nature of a device, let's say in a medical situation where access to that device in an emergency setting, let's say, you need to get in, you need to operate it, and if there are challenges with, let's say, the credentials, what have you, it's one thing that's come up. So I would say maybe, like a lot of things where we operate really in a zone of gray, that's one thing I might just flag. But on balance, you don't want a bad actor to easily commandeer your device.

Mr. HURD. Mr. Corman?

Mr. CORMAN. Just building upon what's been previously said. We looked at the medical device for safety critical emergency access extensively on the congressional task force for the last year and a half. There's a difference between having a hard-coded unchangeable fixed password that adversaries can guess and take advantage of and the ability to go back to a factory default or a safe mode or emergency override with physical access.

So I hear that come up often as an excuse, I'm not saying it's being used that way this time, but no one's saying you shouldn't be able to get to a factory default mode. It's more a matter of are we making it incredibly easy to be herded into a botnet.

And Mirai had to publish its source code after it was done. So even though the first attacks were cameras, one of my first calls was to the Food and Drug Administration to say that the three defining characteristics of Mirai were it was internet facing, it had a fixed password that was guessable, and it was unpatchable. And I just described most connected medical equipment, including half-million-dollar imaging systems and bedside infusion pumpshooked up to people. You can Google these passwords.

So one thing I wanted to clarify is there's a difference between being able to reset them versus how exposed we are with the current condition.

The second thing is, I'm fully onboard with a risk-based decision. It's come up several times. What I want to extend to that, though, and clarify is risk to whom. Because the risk of you buying your internet-based camera is—who cares if your camera gets hacked for you. The risk with the externalities and the tragedy of the commons, that the collective might of all those were able to hurt someone else.

So we should absolutely do risk assessments. But if we narrowly hone in on what's the use case of the buyer as opposed to what's the collective hygiene public health issue of those being herded into a collective might, that must be part of that risk association.

Mr. HURD. Mr. O'Farrell, close out the time that I do not have.

Mr. O'FARRELL. Okay. With respect to the password question, I think if a device needs a password, a hard-coded password effectively means you've no password. So if the device has a password at all, then a hard coded one does not work for that.

Thinking through to devices, yes, on the extreme sensor side of devices, your devices with no operating system, and I would argue, they are not really connected to the internet. They are in turn connected to other systems which connect to the internet, and they're the systems which then need to be protected. But if the device itself is connected to the internet or backed into a data center over TCP/IP or some equivalent protocol, broadly speaking, it will probably have an operating system or at least needs to be protected using a gateway or something else.

Mr. HURD. Thank you.

And we're now round two. Robin Kelly, you're now recognized for your next 5 minutes.

Ms. KELLY. Oh, only five for me, huh. Okay.

There's no doubt in my mind that Congress must establish cybersecurity standards to protect internet-connected devices from hackers and bad actors, but I also understand the other side that, you know, there's concern about rigidly crafted regulations that would stifle innovation.

Mr. O'Farrell, do you believe that the Federal Government can develop IoT cybersecurity without too much stifling of innovation?

Mr. O'FARRELL. So I believe that in the context of the proposal where you're trying to establish what are really pretty basic security rules are basically a kind of a rules of the road for what the Federal Government should be doing for procurement. I think the balance of being able to establish those rules and making sure that you're basically getting value for money against any potential curtailing of innovation, I think is a good balance. These are pretty basic rules. They are not going to some inappropriate level of constraint.

Ms. KELLY. And Mr. Corman had made the comment he thought that the advisory board was a good idea. Do you agree with that assessment?

Mr. O'FARRELL. Yes, I do. I think partially one of the challenges with Internet of Things and anything having to do with cyber moving forward is, as several people have pointed out, you do not know what the threat of tomorrow is going to be and you do not know what adoptive level of security you're goingto have to bring. So an advisory board would help to be able to surface those and react to those before they become a real problem.

Ms. KELLY. Okay. And, Mr. Corman, the Senate version already has the waiver process. Do you think that's a good idea and would ease some concerns?

Mr. CORMAN. To a certain extent. One theory I have is the notion that you can't sell a product with known vulnerabilities unless you get a waiver. I think it'll be the norm that on any given day that you sell you will have some known vulnerability. So we want to make this as streamlined as possible. That's why I err on disclosing, in other words, avoiding a failure to warn. And, you know, the expectation of patching or the ingredients list to know if you need to, even if your vendor doesn't warn you or can't.

So the ability to have a pressure release valve of a waiver process makes sense, because then the agency is explicitly accepting that risk and can do other things to swarm and surround that. But I'd want to make sure that the common path is the easy path is the safe path. And waivers may just be a way to undermine this, so I tend to favor carrot and stick. FDA did something where they essentially said, if you have a disclosure program and you can fix your issue in 30 to 60 days, then you don't have to go through a recall process. Kind of being very clever to say the safe thing is easy thing.

So you can do it however you want, but you're going to want to do it this way. And my only comment on the waivers is let's make sure that they're rare and necessary as opposed to burdensome and slowing down the Federal Government.

Ms. KELLY. And we all know that, as much as we try, no piece of legislation is perfect, so I wanted to give each of you a chance to make a suggestion toward this legislation.

Mr. Eggers?

Mr. EGGERS. Yes, ma'am. Thank you for asking.

I will confess I have not looked at the advisory board idea in detail, but I will. I'm more familiar with the Senate bill. I might even suggest, maybe if there's one thing to take away at least from my thoughts here today, it's that maybe going broader than an advisory board. And what do I mean by that is we found that the Commerce Department can play a really powerful role—NTIA, NIST in particular—to bring multiple stakeholders. The four of us are just a portion of that.

What they can do—and I think the NIST cyber framework effort is a good model. They brought folks together. They're able to say, here's what our interests are. They were consulted. They provided input. There's a lot of back and forth, right? It was quality input-output. I think industry bought it in a major way. We may need to do that here. We are supportive of that.

I think that the Commerce Department—I don't want to speak for them, but I think they would be open to that idea. One thing I might suggest is it's not clear if our friends at NIST and NTIA have the resources they need to carry that forward. One thing I might suggest is we look at what they may need, we may want to consult with them, hey, maybe it doesn't need to be as big as the framework effort where we have about maybe 5 to 6 workshops in the span of about 13 months.

But here's what I took away: Industry played a big role. So did government. Our members bought in, by and large. I can go out, and we do, we promote that framework to about six major chambers, State, local chambers, every year, lead up every year to a summit. So we're able to promote that tool, not only domestically to our businesses, but as a model globally. And that's one of the things we're aiming to, is that we have a process, a model that can work for business wherever they are on the globe. Thank you.

Ms. KELLY. Thank you.

Mr. ROSS. Thank you, Member Kelly. If I might, I'd offer three things. First of all, I think it's a very promising piece of legislation, and, you know, we think the idea of the government using its purchasing power to drive security makes a lot of sense. So these are offered in the spirit of improving that legislation.

Number one, the definition of internet-connected devices, as I've been suggesting, I think needs to reflect risk. And I know that NIST is working on looking at a risk-tiering or a categorization of IoT devices. I think that's maybe something that can be built upon in the definition.

Second of all, I think we really like the emphasis on security research and coordinated vulnerability disclosure. But there are some refinements that we would like to see to make sure that patches can be fully deployed before vulnerabilities are disclosed to the public.

And then the third thing, I'm not sure exactly how you get this in the legislation, but what we would not want to see is any set of standards become sort of the new lowest bar where, you know, that leads to acquisition workforce to buy products that are the cheapest possible as long as they meet the bar. We want to see competition for better cybersecurity and the government buying for value, not just for lowest cost. And I think the more we can do to incentivize that, the better off we'll be.

Ms. KELLY. Thank you.

Mr. CORMAN. I love the question. I appreciate it being asked. Thank you.

I mean, clearly, I proactively mentioned there's tremendous value in a list of ingredients for free market choice at purchase time to tell better products from worse, to answer am I affected and where am I affected, when there's an active attack in the wild that you might be able to actually defend yourself against, and for the devices that have gone out of business, the manufacturers, the ability to defend yourself in those important use cases.

And if I were to add to that, there is a technical standard being discussed called MUD, or Manufacturer Usage Description. It's a very elegant, very simple idea that a device—every device—would advertise to the network this is the man I need to talk to and this is the port I need to speak on. And if other devices in the network noticed it was doing something else, it must be compromised. It's something that on its own may not get as much adoption, but were this part of a government procurement wish list or fast track or incentivized, it could be promising. It's not very robust now, but I like the concept. And it could go even furtherand leverage free market innovation. I think this idea came out of Cisco, if I recall.

And then just a little caution on the disclosure idea, I do agree that great care has to be done on the notion of safe harbor for coordinated vulnerability disclosure. And in my written testimony, I cautioned against MPVD reinventing the wheel. There's been significant and robust debate with the Librarian of Congress, the Copyright Office,who is recommending that the current exemptions to the MCA for research that allowed or enabled the voting machines, medical, to get the strength of law and be made permanent.

I would not want to undo some of those really subtle nuances, nor would I want to tie that to the availability to patch first. There are many devices that cannot be patched, but it's still meaningful to know, to shield yourself, and insulate yourself. So rather than designing that right now, I would be happy to comment further, but I think that that last well-intended suggestion could backfire in unanticipated ways that I could articulate.

Ms. KELLY. Thank you.

Mr. O'FARRELL. Thank you very much for the opportunity to comment on improvements to the bill.

I think I see two areas. One of them is related to the definition of IoT devices themselves. As you can see, it's an area of quite a few questions, but specifically, it points to those IoT devices which are being procured by the Federal Government for use by the Federal Government. I think it would be good to clarify that, if that was to be extended further in some way, that that would be done in cooperation with industry.

So the advisory board, part of that, or even strengthening that in some way to say that we're dealing in this world, which is going to be highly adoptive and highly volatile and, therefore, we need to constantly keep working with industry as we come up with new standards or new rules of the road. I would like to see that incorporated a little bit more strongly in the bill.

Ms. KELLY. Thank you. And I'm done.

Mr. HURD. Mr. Raskin, you're now recognized for an additional 5 minutes.

Mr. RASKIN. Thank you, Mr. Chair.

Ms. Kelly asked one of the questions I wanted to ask and maybe—no, it's an excellent question, Ms. Kelly.

But I did want to ask a similar kind of question which is, at a time when the crises facing the country are multiplying—you know, we had the worst act of mass gun violence, random gun violence in our history a couple days ago; we've got millions of Americans still without power, without water, facing very perilous conditions in Puerto Rico and the Virgin Islands and so on—how would you express to the public the importance and the urgency of what it is you've come to testify about? How would you explain to people why this is something that really requires our attention?

Mr. Eggers?

Mr. EGGERS. Sure. Yes, sir. Thank you.

I think it's pretty simple:We want the IoT to expand and be successful. We think it's going to lead to economic growth and to jobs, but to do that we have to manage risks, smartly. I think that the bill here provides an opportunity for a dialogue around these important issues.

One of the things that we're going to do is we're going to provide the committee, at least I anticipate that we'll do it relatively soon, thoughts on the provisions, at least in the Senate bill, and then we'll move on from there. But I appreciate the opportunity to provide our thoughts.

But I think, if anything, we want to make sure businesses gain as they're producing securely, and so will consumers. But I think we have to manage risks as we expand the IoT. Thank you.

Mr. RASKIN. Anybody else? Mr. Corman?

Mr. CORMAN. One of the lines I put in the Presidential testimony, which was in August last year, has become more true every single day with NotPetya, with WannaCry. And I'm going to read it verbatim. I said: Through our overdependence on undependable things, we have created the condition such that the actions of any outlier can have a profound and asymmetric impact on human life, economic, and national security.

That was a concern of things coming. If you look at healthcare as a sixth of our economy, there's a promise and a peril to these things. But in a sixth of our economy, connected medicine is creating new cures, it's dropping the costs, it's increasing access.

If we are cavalier about risks like this, any crisis of confidence in the public to trust these things could have a very deleterious effect on, not just patient safety, but the economy.

And further, imagine something like the Harlem Presbyterian outage or the WannaCry outage, during a shooting, during a Boston Marathon bombing, during an earthquake or hurricane relief when we need it most. So this is something we have—back to overdependent on undependable IT. Our failure rate is about 100 percent on highly replaceable assets like credit cards. And even though we haven't dramatically improved our cybersecurity on those tolerable losses, we have increased our dependence on these safety critical and national security things.

So without being dire or doom and gloom, we've run out of runway for these low consequence failures. And I think it's not just that we want economic growth, it's that we want the confidence of the public and the national security intact.

Mr. RASKIN. Thank you.

Mr. O'Farrell?

Mr. O'FARRELL. Yeah. Maybe to echo a little bit, I think the reason why this is important is because IT security today is, to a large degree, around privacy or ensuring that financial or other transactions take place securely.

IT security in the context of IoT is going to be around real factories, healthcare, things which directly affect the economy, things that directly affect the day-to-day life within a city. And because of that, compromise or damage associated with those are going to real—and much more impactful in a very, very real way. You have an opportunity to react to a privacy breach of some sort. You do not have an opportunity to react if a factory is brought down or if there's real danger put into a city because of traffic system's been hacked or something like that.

This is why it's important. We're early in the days. IoT is a fledgling story at this stage. So you have an opportunity to build in some security from the very beginning rather than dealing with it after something really bad happens.

Mr. RASKIN. Mr. Ross?

Mr. ROSS. Sir, I would say we can get this wrong in two different directions. One would lead us to lose the benefits of innovation, and the other would lose the benefits of globalization.

You know, it's not just the physical risks that these devices turned against us can pose, it's also losing out on the cutting edge scientific research that these devices are offering or the benefits to public health or the benefits to, you know, critical infrastructure and that kind of thing. And if we don't protect them from cyber attacks, we lose those benefits.

On the other hand, if we go too far and we adopt indigenous standards that put us at odds with the rest of the world, and we close off the internet and we segment and fragment, we lose the ability to transact business around the world and the benefit to our economy that that brings us.

Mr. RASKIN. Thank you.

Mr. Chairman, I also wanted to take a second to thank you for calling this hearing today. Unsecure IoT devices pose significant risk to our national security and can have devastating consequences, as Mr. Corman said. So I think that the Internet of Things Cybersecurity Act is a great first step to protect federally procured IT devices and sensors from cyber attacks.

And I want to thank Representative Kelly for excellent legislation, and I do strongly support her bill.

Mr. HURD. Thank you, Mr. Raskin.

And some final questions from me. How do we prevent—if we say you have to be this tall, from that staying—that that's the floor—or that would be the ceiling, actually, how do we make sure that we continue—that industry continues to follow good digital hygiene?

Mr. CORMAN. We did encounter this at the PCI data security center, the effort to set a minimum, and we got one, right. It almost caused a race to the bottom, and we don't want to cause that.

I think that's why the language we use here is critically important. And I think it's an "and." I don't think it's, do you do in this, private sector, public-private partnership or some minimum hygiene to protect your own interests right now, especially with time being the enemy.

If these thing are evergreen, like never have a password you can't change, we can act on that and we can encourage best practices, carrots and sticks, preferential purchasing, with a parallel effort that does leverage things that can be layered on top of it. It is always a risk. We need to define a minimum that you get it. That's why we have to be very careful, conscientious here that this is something to do the 80/20 rule now. It can't be the finish line.

Mr. HURD. Mr. O'Farrell?

Mr. O'FARRELL. So I don't think we should be afraid to set the minimum. And some of these minimums here are pretty basic and——

Mr. HURD. Pretty minimum, huh?

Mr. O'FARRELL. Pretty minimum. And so we should not be afraid to set those as minimums because we fear, you know, we're not going to be able to do more as it is appropriate. I think the most important thing though, as it is appropriate, does require a lot of interface with industry.

Obviously, I am part of a company who produces a lot of software. I want to be able to have a seat at the table to be able to say, what are the guidelines that we need to follow, how are we going to secure that, and so on. So being involved in that and involving industry is very important. That does not mean we should not be afraid to set this bare minimum, which is, you know, based on what NIST or what some basic cyber hygiene is in place today.

Mr. HURD. Mr. Eggers and Mr. Ross?

Mr. EGGERS. Mr. Chairman, I might just add that I'm always a little concerned, at least I hear concerns expressed from members about minimums and maximums, only because the environment moves so quickly.

One of the things that I think we want to try to do is encourage demand for stronger devices, right. And that may mean that maybe they're more expensive, maybe not. We want makers of devices and those that provide manage services and so forth to gain from that extra security.

One of the things I think about when I start hearing minimums and maximums is, are we in this space going to set some kind of check-the-box formula where it, A, might give us a false sense of security? Maybe with that false sense of security we are not deploying resources optimally. We've seen that happen.

The other thing is, it's not clear where a minimum goes to maybe a higher level. Much depends on the implementation. One thing we have seen is once regulation sort of get going, they are hard to pull back and harmonize. And that's one of the things we're struggling with now.

Mr. HURD. I'm assuming Equifax didn't have a high enough minimum, right? You know, and so we—yes, there should be a—I get the fear. Because my goal is that Congress never gets in the way of entrepreneurship and growth, but it's being made hard when private sector companies are not following basic digital system hygiene. Nobody opted in for their information to be in Equifax, right? And so I get that frustration. But then your members need to get their act together.

Mr. EGGERS. So let me offer a thought. I think you're concerned—I'm not going to argue with your concerns, but here's what I hear from members. So I think one of the things we don't do a good job with is whether it's OPM, SEC, Equifax, and other entity,we're going to have more,we don't do a great job of creating a safe space where an organization can come in as soon as they think that there's something wrong and say, here's what's going on. Rather than having an environment where they're having a finger pointed at them, and you're saying, why did you let this happen,we say, hey, we'll get to that. What can we do to help make things better so we can pull in information, in a voluntary way, and we can learn and get that information out to other organizations?

I honestly haven't learned enough about what's happened with some of these recent breaches to really have a firm sense that I can comfortably say that one organization did very, very poorly and one didn't. I understand that organizations have had challenge, but sometimes we don't know the full picture. And we haven't, at least one thing is, bills like this don't necessarily contemplate what are we going to do about the bad guys, right? What are we going to do about pushing back on bad actors?I think deterrence, at least through denial, stronger devices are some, but what are we also going to do to make an example of bad back actors?So they think, for example, hey, I'm not going to do this again.

Mr. HURD. Mr. Ross?

Mr. ROSS. Mr. Chairman, two points. I think one, you know, we focused a lot on minimum standards today. Part of my suggestion about a risk-based framework is thinking about higher risk devices as well. And, you know, we may decide we don't want to make sure certain devices are patchable or have hard-coded passwords at the very low end. But at the high end, not having a hard-coded password may not be enough. We may want to insist upon two-factor authentication or other identity-management approaches that are much stronger than just not having a hard-coded password. So I think that's one important thing.

The second thing is, if we want minimum standards for government procurement or any other sorts of standards to drive or sort of race to the top for cybersecurity, market mechanisms are really important. And part of that means that consumers, both at the enterprise level and on an individual household basis, need to have information to make informed decisions that factor in security. And right now, we don't have sufficient tools to get information to consumers in ways that they can understand and act upon. So I think that's another really important part of the solution.

Mr. HURD. Mr. Corman.

Mr. CORMAN. You know, I almost wanted to bring up Equifax, but obviously Equifax is not an IoT device. That said, the cause here was a known vulnerability that was able to be remediated but wasn't. It's very similar to this rubric, right? A known but unmitigated vulnerability.

To the point raised just now, though, there is a tongue-in-cheek, much shorter bill we could do, if we want to avoid being prescriptive. We could have a bill that basically says, let the free market do whatever the heck it wants, you are liable for all damages caused by a known vulnerability or a default password.

It's as free market and open to interpretation, as you want. You can be a risk taker, you can be a risk avoider, you can change the cost of goods. A little tongue-in-cheek, but to a certain extent, we have to decide what's reasonable and what's appropriate for the shared responsibility model of the goods that we're inheriting.

So we don't have to necessarily tell them what to do. I think these ones are pretty evergreen, as we've testified thus far. That said, if we want the criteria to change over time, I'dlike to remind everyone listening, not just the committee, this is a statutory authority. I believe we're going to get software liability through case law. I think a jury of their peers is going to find that harm caused to a loved one due to a software defect is no different than harm caused by a physical defect. And we will get case law introducing something, whether or not there's a regulatory or a purchasing procurement document.

So part of the virtue of this particular experiment and this leading by example with procurement guidelines, is I believe, and I said this in my testimony as well, this could create a rubric that could be a safe harbor clause for any case law around this.

So rather than fighting it or wondering what it might do badly, I think it creates a very tenable, intractable building block for the private sector to insulate their harm and insulate their maximum liability. They don't like that at first. I think in the fullness of time, we're going to see this not come through statutory but through case law.

Mr. HURD. Thank you.

Will the gentleman from the Commonwealth of Virginia be interested in asking questions or making comments?

Mr. CONNOLLY. I would. Thank you, Mr. Chairman.

Mr. HURD. And he is recognized for the final 5 minutes.

Mr. CONNOLLY. I thank the CHAIR.

And let me follow up on what you were just saying, Mr. Corman. I take your point, and it may be the way to go. But on the other hand, statutory action influences case law. And not having a statute means that a court in some ways has to itself impose minimum standards if it's going to find liability. And so that's not always a desirable outcome from a legislative point of view.

You may want to comment on that.

Mr. CORMAN. There was a significant discussion on this in the Presidential Commission on Enhancing National Cybersecurity, which did ask the Department of Justice to explore the current state of the law with regards to software liability, just as an uncomfortable truth.

One of the discussions that went in great detail is that if a court is doing this in a vacuum, if they place the liability in the wrong place, it could have devastating effects on the software industry. For example, most of these vulnerabilities that are exploited are in third-party, open-source code that are 100 percent volunteer. So if you were to place responsibility for all the harm caused by Heartbleed when it hit the Federal Government April a few years ago, on the poor guy who introduced the code at 4:00 a.m., on New Year's Day, no one will ever contribute to open source again. And since 90 percent of the software in closed source in commercial goods it's open source, you would have just single handedly destroyed the software industry. And that's not actually a big stretch for a nontechnical jury.

Mr. CONNOLLY. True.

Mr. CORMAN. Yeah.

Mr. CONNOLLY. But, you know, in some of this discussion one would think—let's take Equifax—that it's Equifax that's the victim. Well, 143 million people are also victims. They've had their data compromised. And where do they seek redress?

Your argument that it's a free market, I heard you say, maybe tongue-in-cheek, but an absolute free market doesn't necessarily protect the other victims who've had their financial information compromised.

Mr. CORMAN. It's my sincere belief that a few years from now, whether we chose to do it or are forced to do it, we're going to end up with a rubric that people are not responsible for zero day attacks from China, but they are absolutely responsible for known avoidable vulnerabilities. I think everything is going to hinge on what was known and avoidable.

Mr. CONNOLLY. Well, you know, GAO in a series of reports basically found, and I quote: "While there are many industry-specific standards and best practices that address information security, standards and best practices specific to IoT technologies are still in development and not widely adopted."

Now, Congress, generally in this sphere, has been reluctant to legislate, actually. Some would criticize us for being too reluctant. But that kind of finding suggests, as the chairman I think was indicating, either industry adopt some industry-wide standards that people can adhere to that give us some comfort in protecting the citizens we represent, or we have to do it.

Mr. Ross.

Mr. ROSS. Congressman, if I might. I think it's a great point. I think we will get maximum bang for the buck when those standards are international standards, because so many devices are produced overseas. And I think there is a gap. There's a gap, for example, you know, there is a proliferation of different types of operating systems for IoT devices, and that has a real impact on their security. Having a—you know, having international standards around IoT operating systems might be something we ought to explore. And I think the government can play a big role in supporting efforts to develop international standards.

And that's something we haven't looked at nearly enough, in my view, because, you know, a lot of times international standards are developed on the side by people who, you know, work in the industry and try to come up with an international standard in their free time. That can't be how we approach security. We need a much more focused approach on identifying where there are gaps or where standards are out of date and really putting some support behind developing them in the international context.

Mr. CONNOLLY. And that's a good point. I would just say, keep in mind that if this isn't done with some robustness by the private sector, sooner or later the public sector will be under enormous pressure. For example, if there ever is something that we kind of agree is a cyber Pearl Harbor, the shutdown of the electric grid, or the banking system, writ large, the public pressure on us to do something will be enormous.

And so some sense of urgency, it seems to me, is really important within the private sector to get some kind of basic standards that people buy into that are reassuring, that aren't just, you know, PR, but that actually provide some protection that is measurable and testable.

Absent that, I fear that some day it will be done for you, because the pressure will be so great after some incident, Equifax apparently isn't it, but it was big enough that it got a lot of attention. And I just fear that when that day comes, absent private sector activity, you're going to see tremendous pressure on the legislative branch to protect the public.

Mr. ROSS. Congressman, I fear that too. I think the one thing I would say is that it doesn't necessarily have to be the private sector taking action versus the public sector, but the private sector and the public sector working together is really powerful. And I think what we've seen, you know, within this framework is that industry and government got together on a framework that has proved very valuable by all accounts. But it's now, you know, the government and the private sector together are also now taking it to the International Organization of Standardization and seeking to internationalize it as a standard. And I think that's a great model for how we can explore IoT cybersecurity, but also other areas where we really need to fill in the gaps on international standardization for security.

Mr. CONNOLLY. And I know my time is up, but I would agree with you. I think that's a preferable way to go, but it's got to be robust, it's got to be measurable and testable, it's got to be reassuring to the public and most of the stakeholders. Otherwise when something happens, that will be found to have been as inadequate as it is.

Mr. ROSS. Absolutely.

Mr. CONNOLLY. I thank the chair.

Mr. HURD. Thank you, sir.

And I'd like to thank our panel of witnesses today. This really was an invaluable conversation. I always feel when I leave a hearing with just as many questions as answers, it's actually a good thing. And so thanks for taking the time,thanks for y'all's perspective.

And the hearing record will remain open for 2 weeks for any member to submit a written opening statement or questions for the record.

And if there's no further business, without objection, the subcommittee stands adjourned.

[Whereupon, at 4:08 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Cybersecurity of the Internet of Things

House Committee on Oversight and Government Reform

Subcommittee on Information Technology

2:00 PM, Tuesday, October 3, 2017

2247 RHOB

Rep. Gerald E. Connolly (D-VA)

Thank you, Mr. Chairman for holding this hearing to examine the federal government's role in creating policies to ensure the security of internet-connected devices, or the Internet of Things (IoT), while still allowing for innovation and growth.

From cell phones to baby monitors to watches, IoT devices and the data they transmit already present enormous benefits to consumers. Federal, state, and local governments can also take advantage of the Internet of Things to be more efficient and deliver better customer service to their residents.

The rapidly expanding Internet of Things technology presents many security challenges as well. The technology research company, Gartner, estimates that by 2020, there will be more than 20 billion IoT devices. Each of these devices is a potential entry point for a cyber-attack. These devices can be taken over to do something they are not intended to do, like a smart refrigerator that becomes part of a botnet attack. These devices can also be hijacked to do what they are intended to do, but in a harmful way. Two years ago, Wired magazine documented how two security researchers were able to hack into an Internet connected car and control its air-conditioning, radio, and windshield wipers.[1] These two researchers were even able cut the car's transmission, slowing it to a crawl on a St. Louis highway.

As the use of internet-connected devices continues to increase, so will cyber-attacks targeting these devices. Yet there are no current minimum-security requirements for IoT devices. GAO has found that the growth and adoption of increasingly less-expensive IoT technologies

[1] Wired Magazine, *Hackers Remotely Kill A Jeep On The Highway – With Me In It (July 21, 2015) (online at* https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway).

pose security risks to federal departments and agencies, emerging smart-cities, the individual personal privacy of American citizens, and our national security.

One of the reasons why IoT devices have such low security is because designers want to make these devices as simple as possible, often sacrificing security. The Internet of Things Cybersecurity Improvement Act (S.1691) introduced in the Senate addresses the lack of standards for IoT devices sold to the Federal government. The legislation requires that such devices have the ability to be patched and have passwords that can be changed by the users. The bill would also prohibit Federal agencies and departments from acquiring IoT devices with known security flaws and would require device makers to patch any new issues. While this legislation would not solve all IoT related security concerns, it sets a commonsense baseline that will hopefully push IoT device manufactures to consider basic security when putting these items on the market.

There are also several steps this Administration can take to address the cybersecurity threats facing the Federal government. First, the President should appoint a Federal Chief Information Officer. It is irresponsible that this Administration has not appointed a Federal CIO to lead the government's approach to acquiring and managing all of its IT investments. It is also incomprehensible, that at a time of increased cyber threats, the Administration has not only left the Chief Information Security Officer – or CISO – position vacant but has appointed the Deputy CISO to be both the Acting CISO as well as a Senior Director on the National Security Council's cybersecurity team. Assigning one person to do the job of three people does not send the message that cyber security is a priority for this Administration. I urge this Administration to make key appointments at the Office of Management and Budget as well as federal agencies to ensure that the government is well-equipped to address all cyber risks.

Given the rapid expansion of IoT technologies and the increased use of IoT devices for everyday activities, it is important that security issues are addressed before the challenge becomes too complicated and costly. I look forward to hearing from our witnesses their views on what Congress can do to address the cyber risks presented by IoT technologies and devices.

Matthew J. Eggers
Executive Director, Cybersecurity Policy, U.S. Chamber of Commerce
House Oversight and Government Reform Committee, Information Technology Subcommittee
October 3, 2017, Hearing, *Cybersecurity of the Internet of Things*
November 15, 2017, Questions for the Record

Mr. Corman called for a "software bill of materials" in his testimony to empower agencies to be better informed in the procurement process, help evaluate a new vulnerability's effect and, be aware when the product expirers. Please share your thoughts on feasibility, effectiveness, and challenges with this idea.

The U.S. Chamber of Commerce shares policymakers' goal to help the federal government buy secure internet-connected devices. Many companies go to great lengths to incorporate security into the design phase of IoT devices and services they sell globally. Still, public and private sector stakeholders realize that the Internet of Things (IoT) marketplace is not fully mature, including with respect to cybersecurity. Securing the IoT must be a top U.S. objective.

Indeed, the Chamber believes that the business community needs to lead the development of secure and resilient devices with positive, nonregulatory support from policymakers. We advocated this view on October 3 at the IT subcommittee hearing *Cybersecurity of the Internet of Things*; on October 19 at a National Institute of Standards and Technology (NIST) colloquium on IoT cybersecurity;[1] and through the Chamber's national cybersecurity education campaign, among other settings.[2]

IoT cybersecurity proposals such as a software bill of materials, aka a label, need to proceed carefully, including how such efforts are developed and implemented.[3] First, stakeholders should not push a one-size-fits-all approach to addressing IoT cybersecurity labelling. Pacemakers and dishwashers clearly have different uses and unique risk environments. The IoT is incredibly complex, and there is no silver bullet to cybersecurity.

Second, the Chamber largely agrees with the National Telecommunications and Information Administration's (NTIA's) apparent thinking that a label, which could provide an inventory list of ingredients for third-party software components, needs to be implemented *from the ground up in a voluntary fashion.* Done this way, a label could help developers understand the software code that goes into their products and purchasers understand exactly what's in the

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

[2] The Chamber has spearheaded some 16 major regional roundtables and three summits in Washington, D.C., since 2014. More events are planned for 2018. The Chamber's *Sixth Annual Cybersecurity Summit* was held on October 4, 2017. Each regional event includes approximately 200 attendees and typically features cyber principals from the White House, the Department of Homeland Security, the National Institute of Standards and Technology, and local FBI and Secret Service officials.

[3] www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

products they are buying.[4] Transparency for its own sake is not the goal. Labelling data must be useful to enterprises that make devices and the organizations that buy them. Strong IoT security should be a win-win proposition for makers, providers, and purchasers.

The Chamber generally supports the position of BSA | The Software Alliance, which calls for driving IoT cybersecurity through adoption of software security best practices. The association backs the widespread integration of security-by-design principles into IoT standards and guidance, including secure software development life cycles that help organizations assess and mitigate risk in their supply chains.[5]

Third, top-down, government mandates on labelling could trigger a backlash against American firms. Governments around the world closely watch U.S. policymaking, and a new law could prompt foreign magistrates to enact similar programs as a condition of sale into their markets. In August 2017, the Chamber's Global Information Security Working Group 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.[6] Ultimately, IoT cyber solutions must come from the marketplace. Governments should not dictate device security but catalyze solutions that industry shapes and advocates at home and abroad.

In the immediate term, what are some steps that agencies could, or should, take now to educate within and promote basic cyber hygiene practices in relation to the Internet of Things? What should we be looking at in addition to endpoint devices?

The Chamber principally urges Congress and the Trump administration to fund a multistakeholder effort, led by the Department of Commerce, on IoT cybersecurity comparable to the NIST Cybersecurity Framework (Framework) before advancing IoT legislation (e.g., smart cities, connected devices, and labels). There are valuable lessons underpinning the Chamber's enthusiasm for the Framework process, which could apply to an IoT cybersecurity framework or architecture initiative.

[4] "NTIA, in review of comments on botnet strategy, cites calls for security 'certification,'" *Inside Cybersecurity*, September 19, 2017.
https://insidecybersecurity.com/daily-news/ntia-review-comments-botnet-strategy-cites-calls-security-certification

[5] www.bsa.org/~/media/Files/Policy/BSA_2017CybersecurityAgenda.pdf

[6] See August 16, 2017, letter to the 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

First, NIST did an admirable job convening many organizations to develop the Framework over the course of many months. Second, businesses view the Framework as a pillar for managing enterprise cyber risks and threats, including at home and increasingly abroad. Third, the Framework has strong bipartisan support on Capitol Hill and in the current and previous administrations, which is not something that industry takes for granted.

The Chamber is urging the Trump administration to embrace the Framework domestically and internationally.[7] We see the Framework as a technically sound tool, a collaborative process, and a mind-set committed to managing risk. The Chamber urges private organizations—from the C-suite to the newest hire—to dedicate themselves to robust cybersecurity practices and regular improvements.[8] Just as the Framework enables businesses to account for cybersecurity beyond their own enterprises, an IoT cyber architecture will help businesses think about the security and resilience of their networks and supply chains, not just their IoT devices.

Federal agencies are working to bridge education gaps through the National Initiative for Cybersecurity Education, or NICE, which involves many government entities.[9] Agencies are pursuing proactive education activities, such as publishing guidance by the Department of Transportation's National Highway Traffic Safety Administration[10] and blogs by the Federal Trade Commission,[11] which are targeted to the agencies' stakeholders. The Food and Drug Administration has published papers that feature recommendations for comprehensive management of medical device cyber risks throughout the product life cycle.[12] These agency initiatives must remain dynamic and nonregulatory if they are to be collaborative vis-à-vis the business community.

How would you envision that IoT devices comply with the NIST database that contains over 90,000 vulnerabilities and is growing day by day?

The Chamber requests that the IT subcommittee add our accompanying paper *Preliminary Feedback on S. 1691, the Internet of Things (IoT) Cybersecurity Improvement Act of 2017* to the hearing record. The legislation deserves scrutiny through constructive dialogue.

[7] www.uschamber.com/press-release/us-chamber-report-offers-framework-us-eu-cybersecurity-cooperation

[8] www.uschamber.com/sites/default/files/u.s._chamber_letter_nist-wh_cyber_commission_rfi_sept._9_final_v2.1.pdf, www.uschamber.com/sites/default/files/documents/files/industry_comment_ltr_to_european_commission_on_future_of_public_private_partnerships.pdf

[9] www.ntia.doc.gov/files/ntia/publications/rfc_comment_summary_20170918.pdf

[10] www.nhtsa.gov/press-releases/us-dot-issues-federal-guidance-automotive-industry-improving-motor-vehicle

[11] www.ftc.gov/tips-advice/business-center, www.ftc.gov/iot-home-inspector-challenge

[12] https://blogs.fda.gov/fdavoice/index.php/2017/10/fdas-role-in-medical-device-cybersecurity

Among other things, it establishes new federal mandates for how companies develop their software and internet-connected devices through the imposition of requirements on government contractors. The Chamber supports robust device security and resilience, but the bill raises several concerns about how agencies—led by the Office of Management and Budget in consultation with others—would write guidelines and practically implement them.

In general, S. 1691 takes a broad-brush approach to addressing federal IoT cybersecurity. It doesn't distinguish among the extraordinary array of devices covered under the bill based on their types and unique risk environments. In other words, the legislation would impact every internet-connected item in roughly the same manner (e.g., military mission-critical devices would be treated the same as connected dishwashers purchased by agencies).

The bill's vulnerability notification regime concerning device vulnerabilities could easily become unwieldy, and disclosure should not become an end in itself. Even some security researchers who are proponents of vulnerability disclosure programs argue that S. 1691 creates unrealistic expectations for contractors. Four provisions in the legislation that pertain to vulnerabilities and warrant scrutiny are as follows:

- **Pg. 3, lines 22–25, sec. 2(9)** The definition of "security vulnerability" is overly expansive. The definition encompasses known vulnerabilities in the device and "any attribute of hardware, firmware, software, process, or procedure or combination of 2 or more of these factors" that could defeat an information system or a device. It is practically impossible for a contractor to anticipate the myriad ways a government customer will use a device, which can trigger and/or reveal the existence of previously unknown vulnerabilities, thus increasing contractors' notification workload.

- **Pg. 5, lines 5–18, sec. 3(a)(1)(A)** The legislation insufficiently explains what "known security vulnerabilities" would capture. While S. 1691 defines a vulnerability as "known" if listed in NIST's National Vulnerability Database (NVD), the bill would also authorize the selection of another—yet to be selected—database by the OMB. Such language makes "known security vulnerabilities" difficult to interpret with precision.

  Contractors strive to weed out most vulnerabilities by using commercially sound practices for delivering robust IoT products to the marketplace. If bill writers use the NVD, the legislation should specify a severity threshold. Setting a severity ranking of "Low" will generate much noise and become an unreasonable burden for contractors to comply with the bill's certification requirements. Agencies, too, will be encumbered by the need to evaluate a potential flood of incoming vulnerability data that are not useable.

  Under S. 1691, contractors would need to police all vulnerabilities in devices that they market to agencies. The list of sources (e.g., customers, distributors, media, researchers, and domestic and international CERTs) that contractors would need to monitor for vulnerabilities is lengthy and runs contrary to prudent risk management practices. Vulnerabilities do not need to be mitigated equally, which the legislation's writers appreciate, but this thinking (aside from waivers) is not sufficiently evident in the bill.

- **Pg. 5, line 13, sec. 3(a)(1)(A)(i)(I)(bb)** The bill provides for maintaining a public database (i.e., see "any additional database . . . that tracks security vulnerabilities") of devices procured by agencies. However, the Chamber is concerned that creating a device directory is potentially unwise and could provide a path for nefarious actors to exploit. What's more, a "publicly accessible database" would also list devices whose security support has ended, helping further spotlight targets for malicious hackers.

- **Pg. 6, lines 11–20, sec. 3(a)(1)(A)(ii)** S. 1691 would seemingly grant limited exceptions (i.e., waivers) to contractors that supply devices to the government with known vulnerabilities. Contractors must explain to the agencies why the device should be considered secure and provide a description of any "mitigating actions" employed to limit the exploitability of the vulnerability.

  Many factors go into deciding when and how businesses disclose vulnerabilities in a device, particularly if the weaknesses affect multiple products or are comparatively severe in nature. Software vulnerabilities are often disclosed in cooperation with US-CERT. The existing public-private disclosure system frequently gives stakeholders the opportunity to implement compensating controls until a vulnerability patch is developed and deployed.

  However, section 3 of the bill could lessen the likelihood of early voluntary disclosures by contractors. Contractors may be unable to bid on proposals unless waiver applications are granted for devices with known vulnerabilities. Penalizing companies for researching and disclosing vulnerabilities is in no one's interest. The bill could have the unintended consequence of reducing voluntary disclosures, thereby upending a key element of U.S. and international cybersecurity best practices. Sometimes it's in the public interest for a vulnerability to be disclosed before it can be patched, and sometimes it isn't because of reasonable risk management determinations.

  Complicating matters further, parts of the U.S. government have a history of weaponizing vulnerabilities for clandestine and covert programs that, while understandable, can significantly dampen industry's willingness to voluntarily disclose vulnerabilities to the government.

- **Pg. 7, lines 19–24; pg. 8, lines 1–2; sec. 3(a)(1)(B)** The "Notification Required" clause requires a contractor to disclose to the purchasing agency both vulnerabilities reported by an external researcher and vulnerabilities or defects "which the vendor otherwise becomes aware of for the duration of the contract," which is sweeping. The House OGR IT Subcommittee hearing in October highlighted that it's probable complex cyber systems will have several vulnerabilities over the course of a year.

Tommy Ross
Senior Director, Policy
BSA | The Software Alliance
Questions for the Record
Subcommittee on Information Technology
House Committee on Oversight and Government Reform

Mr. Corman called for a "software bill of materials" in his testimony to empower agencies to be better informed in the procurement process, aid in evaluating a new vulnerability's effect and awareness of when product support expires. Please share your thoughts on feasibility, effectiveness, and challenges with this idea.

BSA's newly released cybersecurity policy agenda, "A Cybersecurity Agenda for the Connected Age," advocates the development of tools to communicate critical cybersecurity information to consumers and enterprise stakeholders, and the concept of a "software bill of materials" is deserving of consideration as such a tool. The potential efficacy of the concept will depend upon how key details are resolved, such as the specific content and format of such a label.

In general, such tools should be evaluated based on whether they provide individual and enterprise consumers with information that is *actionable*; that is, information that is intelligible to the intended audience and provides a basis for making informed decisions about products on the basis of security characteristics. As I understand the proposal for a software bill of materials, such a label, inasmuch as it would include a list of components used within a software product, may not be easily digestible by average consumers, including many enterprise consumers, who may not have the ability to analyze or distinguish between such components. It may have more value for sophisticated enterprise consumers; alternatively, it may be more valuable as part of a digital tag that could communicate with network management hubs, as some have proposed. As noted, the value will depend on the details of such a concept.

Tools must also be *viable* from a business standpoint; that is, implementable without creating impractical or overly burdensome requirements for covered businesses. Software often comprises multiple components, both proprietary and open source, often from multiple sources within a supply chain. BSA strongly supports widespread adoption of security-by-design principles, including secure software development lifecycles, which facilitate supply chain transparency and accountability. Nevertheless, it would be important that a software bill of materials, if widely adopted, avoid necessitating development processes that significantly increase cost and complexity or unnecessarily hamper innovation and speed.

Discussions about a software bill of materials continue to evolve, and much work remains to be done to define key details. BSA is eager to see these discussions advance to contribute to tools that are viable and provide actionable information to consumers at the individual and enterprise levels to drive stronger cybersecurity.

In the immediate term, what are some steps that agencies could, or should, be taking now to educate within and promote basic cyber hygiene practices in relation to the Internet of Things? What should we be looking at in addition to end point devices?

Cyber hygiene is a challenge within the government as much as it is for the public at large; in both contexts, malicious cyber actors commonly take advantage of poor individual and, in some cases, enterprise practices for maintaining basic cyber hygiene. Basic cyber hygiene education within government agencies can go a long way not only to defend government networks but also to set an example for the broader public. As such, regular trainings on cyber hygiene, as already conducted by many agencies, and awareness events such as National Cybersecurity Awareness Month, can pay important dividends.

Beyond education, there is much the government can do. BSA strongly supports the direction provided through President Trump's Executive Order on cybersecurity, issued earlier this year, that all government agencies develop risk management plans consistent with the National Institute for Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity.* In addition, the federal government should consider the following measures to improve basic cyber hygiene across government agencies:

(1) Invest in cybersecurity through modernizing technology. BSA strongly supports efforts by Congress and the Administration to modernize the Government's information technology systems, and advocates for government agencies to invest in systems that adopt strong cybersecurity measures as part of this modernization.
(2) Strengthen identity management. Government agencies can address one of the most persistent cyber hygiene challenges – safeguarding identity – by encouraging and investing in cutting-edge identity management technologies. Such technologies should not only be used for authenticating and governing access to government employees, but should also be deployed for use on government portals through which citizens provide personal data.
(3) Improve the exchange of cybersecurity professionals between the government and private sector. Enhanced opportunities for private sector cybersecurity experts to join the government for periodic or short-term assignments can improve cyber hygiene by providing government agencies with greater exposure and access to the expertise of leading cybersecurity practitioners.

How would you envision IoT devices to comply with the NIST database that contains over 90,000 vulnerabilities and growing day-by-day?

Not all vulnerabilities are created equal, and not all vulnerabilities necessarily heighten insecurity. Many software developers already use processes, such as secure software development lifecycle approaches or Agile methods, or tools, such as those developed by the Software Engineering Institute's Secure Coding Initiative, to develop strong, secure code and limit use of known vulnerabilities. These practices should be encouraged.

However, across-the-board bans on the use of software containing vulnerabilities listed in the NIST vulnerability database may be unnecessary and counterproductive. Some code segments listed as known vulnerabilities may be used as part of a broader code base that incorporates mitigations against the known vulnerability, and it makes little sense to erect barriers against the use of such software. Two alternative approaches may make more sense. First, rather than an across-the-board ban of known vulnerabilities, software developers could be asked to certify that their software contains no known *and* unmitigated vulnerabilities. A second constructive approach may be to encourage adoption of relevant international standards, such as ISO/IEC 27034. These outcome-focused approaches would allow software engineers the flexibility to achieve the best solution for a particular software requirement while ensuring that software vulnerabilities are identified and mitigated during the development phase.

(QFRs) Questions For the Record for Statement of Joshua Corman

For the House Oversight and Government Reform Committee's Subcommittee on Information Technology "Cybersecurity of the Internet of Things"

Oct 03, 2017

QFR #1:
Question: In the immediate term, what are some steps that agencies could, or should, be taking now to educate within and promote basic cyber hygiene practices in relation to the Internet of Things? What should we be looking at in addition to the end point devices?

Answer #1:
There are a few parallel efforts that can be undertaken while the proposed legislation is being debated and implemented. I'll list a few high-level thoughts on:

A) Education/Awareness
B) Principles for more conscientious dependence or adoption
C) Technical mitigation approaches

1A) Education/Awareness:
There is an (as of yet) unwarranted (and unsound) "implicit trust" in connected technology. For a moment, think of the lengths we used to go through to avoid "bugs" and listening or tracking devices - for our privacy and national security. Now think about how many appliances, toys, or gadgets we have in our home or our offices which capture and transmit audio (or even video), our locations, our preferences.

I've found these default mindsets and beliefs are some of the biggest liabilities to the safe and secure embrace of connected technology. Via "I am The Cavalry", I've had some success with a few phrases like:

"With great connectivity, comes great responsibility."

"If you can't afford to protect it, then you can't afford to connect it.

"If you add software to something, you make it vulnerable. If you add connectivity, you make it exposed – exposing ourselves to a bevy of accidents & adversaries."

"Our dependence on connected technology is growing faster than our ability

to secure it – in areas affecting public safety and human life."

"Through our over dependence on undependable IT, we have created the conditions such that the actions of any single outlier can have a profound and asymmetric impact on human life, economic, and national security."

I've often wondered if "I am The Cavalry" could partner with the US Government to do a concerted IoT / Cyber Safety Education and Awareness Campaign. My preference was to do a modern spin on US WW2 Posters, or a re-boot of the classic "School House Rocks" cartoons on how government works: "I'm just a bill...". Another motif could be to fashion PSAs in a style like the *Truth.org* anti-smoking pieces.

The US Government already does National Cybersecurity Awareness Month in October (and *"Stop. Think. Connect."*), and I had proposed an extension for Safety Critical IoT – or even making November (or another month) National Cyber SAFETY Awareness Month. In fact, this sentiment is supported by the December 2016 Report by the *Presidential Commission on Enhancing National Cybersecurity* where it called for a more modern and continuous set of education to inform and empower the public and market forces (demand).

1B) Principles for more conscientious dependence or adoption:
To this end, "I am The Cavalry" has developed and published three very simple, accessible, multi-stakeholder frameworks to catalyze progress and transparency – as our society shifts from "current state" to "desired state" of safe, dependable, and trustworthy IoT.

5 Star Automotive: https://www.iamthecavalry.org/5star/
Hippocratic Oath for Medical Devices: https://www.iamthecavalry.org/oath/
6 differences in Safety Critical IoT: https://www.iamthecavalry.org/iotdifferences

Our first of these was a **"Five Star Automotive Cyber Safety Framework"** on August 8th of 2014. Second, we later published a similar one for Medical Devices on January 19th of 2016 called a **"Hippocratic Oath for Connected Medical Devices"**. Both acknowledge that "All systems fail" and in the face of this truth, safety critical IoT should be prepared for failure across 5 dimensions: How do you:

- Avoid **failure** (Cyber Safety by Design)
- Take help avoiding **failure** (Coordinated Vulnerability Disclosure Programs)
- Capture, study, and learn from **failure (**Evidence Capture)
- Contain & isolate **failure** (Segmentation of Critical from Non-Critical)
- Respond quickly to **failure** (Security Updates/Patches)

Third, while both of these have been useful for the complex, multi-stakeholder markets they aim to serve, we have also had significant success with defenders, enterprises, and government agencies with a **"six differences"** framework articulating how Safety Critical and IoT are different than traditional cybersecurity assumptions and "best practices". These six dimensions can help temper/enhance popular frameworks like the NIST CSF (Cyber Security Framework). Executive branch agencies would be well served to scrutinize selection and deployment by asking questions across all of these differences in:

- ***Adversaries***: Motivations, Objectives, Capabilities, Will
- ***Consequences of Failure***: Life & Limb, Physical Damage, Market Stability, GDP, International and National Security
- ***Context & Environments***: Operational differences, Migratory, Perimeter-less, Inaccessible, Difficult to Patch/Replace
- ***Composition of Goods***: Hardware, Firmware, Software
- ***Economics***: Margins, Buyers, Investors, Costs of Goods, Regulatory, Depreciation
- ***Time Scales***: Time-to-Live (TTL), R&D Cycles, Response Times

1C) Technical mitigation approaches

This bill seeks to make the IoT devices themselves more secure and defensible. We often advocate that it is better when security is **"Built-In versus Bolt-on"**. That said, there will always be a role for Bolt-On and after-market assistance. Too often these aftermarket network and endpoint controls are less fit for purpose, they are expensive to buy, operate, and maintain – and may even be the target of compromise. Further, approaches to protect confidentiality of data assets are ill fit for purpose to protect confidentiality and integrity of human life.

Here are some deployment/mitigation thoughts for the QFR question of "immediate term":

- Do I need a connected X or Smart X? or is it too much risk?
- If we already bought a connected X, can we disable the connectivity?
- If we must connect the device:
    - can we harden its configuration to be less prone?
    - can the default passwords be changed - and have we done so?
    - can the software be patched/updated - and have we done so?
    - can we use network and/or wireless isolation/segmentation to insulate other, more sensitive systems?
        - E.g a Dedicated, untrusted IoT wireless hotspot or Network
    - can we shield these devices with forms of NETWORK security such as:
        - Firewalls (FW)
        - NextGen Firewalls (NGFW – akak Application Aware Firewall)
        - Intrusion Detection and Prevention Systems (IDS/IPS)
        - Unified Threat Management (UTM – often a combo of several above)
        - Web Application Firewalls (WAF)
        - Network Admission Control (NAC)
        - Network Behavioral Anomaly Detection (NBAD)
    - can we shield these devices with forms of ENDPOINT security like we see on PC's – like Anti-Virus – while recognizing that:
        - Most offerings don't (or won't) exist for the various IoT hardware, firmware, software combinations
        - Most low cost IoT lacks the compute power to do these
        - We also think it is a terrible idea that we'd put Anti-Virus type complexity and costs on our fridges, TVs, coffee makers, vending machines, and the like.

Another risk and operational issue is even knowing which IoT you may have in your environment. There are some solutions that passively monitor network segments and can fingerprint device types. These have costs and are not comprehensive. That said, they may be useful in some agencies and networks.

A key objective every agency should have is to populate and maintain and inventory of all of the systems – IoT or otherwise. Such inventories are key for many IT and Security uses cases including=, but not limited to: patching, impact analysis (Am I affected by this new attack? – and where am I affected?)

QFR #2:
Question: How would you envision IoT device to comply with NIST database that contains over 90,000 vulnerabilities and growing day-by-day?

***Answer #2*:**
There a few layers and aspects to answering this question. Given the phrasing, the question implies this task may be onerous. I will attempt to break this down and explain:

A) why it is less onerous than one might think
B) why it must be dynamic, automated, and ongoing (and can be)
C) why it is reasonable
D) why it is more valuable than one might think (beyond security reasons)

2A) Less Onerous:
I hope no one thinks someone would manually execute 90,000+ exploits sequentially. How one determines exposure to Common Vulnerabilities and Exposures (CVEs) in the NVD (NIST's National Vulnerability Database) can (and should) be approached in an intelligent and scalable manner. For any given IoT device, only a fraction of all known vulnerabilities will be in play. For example, if the IoT device is not running Microsoft Windows that entire swath of CVEs will not apply to them.

It is important to state that many organizations already manage their software supply chain hygiene incredibly well (including tracking vulnerabilities added to NVD and several other databases, to see if they're affected and where they're affected, across their software/product portfolio) - and at scale. This is not a theory, this is a practice – it just isn't universally adopted yet (but should be). These organizations do this for a number of non-security reasons – in addition to the security benefits. Over the last 4 years, I have personally helped banks, retailers, medical device makers, and other firms voluntarily drive these programs. It is an even more common practice in development organizations who do DevOps and Continuous Delivery (such a Netflix, Twitter, Google, tier 1 banks, retailers, and other leaders in this space). These principles have been promoted aggressively in the FS-ISAC (Financial Services) now for at least four years.

2B) Dynamic, Automated, and Ongoing:
Computers and automation are really good at doing this sort of thing – if equipped.

In both my written and oral testimony, I called out the bill would be significantly stronger if it included a software Bill of Materials (BoM) which lists all 3rd party and open source software components (parts) with their version numbers. Even if never published or shared, the BoM supports and enables ongoing and automated assessment of exposure to vulnerabilities – for the life of that product or version of product.

A BoM is one of the easiest and most scalable assessment methods to start with. If one knows which components are involved in its products, those parts and versions can be cross-referenced with the NVD – programmatically and even perpetually (in cases where a company has gone out of business or the product is no longer supported). This can be done for free with scripts and NVD queries. This can be done with free tools like OWASPs Dependency Checker. This can be done with commercial tools like Black Duck, Sonatype, SourceClear, VeraCode, and others. Where/when this can be (and is) done is either: scanning binary repositories (like Nexus or Artifactory), as almost a spell checker in development tools (IDEs like Eclipse or IntelliJ), in software integration/build servers (like Jenkins), or by scanning/fingerprinting completed products after the fact.

Outside of software BoMs, there are also vulnerability scanning tools (both free and commercial) which can attempt to enumerate vulnerabilities in products. These vulnerability scanning tools are certainly a part of a good secure software development life cycle (SDLC) and work well within NIST's Cyber Security Framework, but on their own these tend to be inferior to approach for several reasons. One is that they tend to not create checks for all CVEs – and they tend to miss many of the CVEs they do attempt. Another is the scans can be time consuming. Another reason is they only tell you what they know to be bad - at the moment they scan – with the checks they have at that moment. Some analysis I saw showed some commercial scanners only write checks for about half of CVE – and only catch about half of what they check for.

In contrast, a software Bill of Materials can be perpetually queried for known associated CVEs against those versions. New CVEs are constantly revealed, so the list of known vulnerabilities is and will be dynamic. The fastest and least invasive way to automate this is to routinely script a cross reference of known parts (SW BoM) to known vulnerabilities (NVD CVEs).

The Equifax breach was not IoT, but may serve as a good example. Equifax was breached with a known vulnerability in some versions of Apache Struts2. If a Bill of Materials listed Equifax's version of Apache Struts 2, then scripts and tools could query NVD to identify the CVEs associated with that version – and alert them to take remediation – before harm. If you don't know what you're dependent upon, you can't defend yourself.

2C) Reasonable:

With the volume and variety of new vulnerabilities – as well as the velocity with which they are exploited – it is imperative that IoT devices are prepared for this new normal. The bill outlines reasonable hygiene steps that are being done by some - and can be done by others.

While some vendors have complained that it is unreasonable to avoid known vulnerabilities (or even to at least know and disclose them), I'd argue a failure to do even this minimal level of transparency is unreasonable. A few thoughts:

A vendor who doesn't even know their own supply chain or hygiene, gives me significantly less confidence than one who does know. Tax Payer dollars should be driven toward the best and most reliable supplier and offerings. We cannot afford the next OPM breach to be due to a 10 year old, entirely avoidable vulnerability, in a low cost IoT device. We don't say "eat at your own risk" on food. We list ingredients, potential allergies, and nutritional information. These transparency mechanisms support informed, free market choice.

The ability to assess the relative hygiene of product/vendors "A, B, and C" allows me to better select where to place my money and trust, how to assess cost of ownership, how to factor additional risk mitigations which will be required, etc.

From a legal perspective, a vendor who has vulnerabilities, but fails to share them, puts dependent customers and consumers in an untenable position. There is a strong argument this could constitute a "failure to warn".

When combined with the lack of any liability for software defects, manufacturers can pass defects on to their customers, not warn them of those defects, and hold no responsibility for those harms caused by the defects they passed silently onto their customers. This is especially egregious when it comes to public safety, human life, and national security levels of consequences – in the internet of everything.

The rubric of this bill, doesn't ask for perfect software – or immunity against unknown, nation state level vulnerabilities. It expects that known vulnerabilities are: avoided, disclosed when they can't be, patchable, and encourages proactive "good guy" discovery and resolution through coordinated vulnerability disclosure. The lifecycle around known vulnerabilities is more reasonable, more tractable, and in many ways more valuable – as known vulnerabilities are significantly more likely to be exploited and attacked in the wild and at scale.

If we invert this, is it reasonable? ...
to sell a device that is vulnerable (with a 5+ year old vulnerability), un-patchable, and the device maker shouldn't have to know that or tell you that – nor are they responsible for harm that you experience from those undisclosed defects. Is that reasonable?

Further, no one has to comply with the bill. They can either choose not to sell to the federal government, or they can choose to pursue a waiver – as the bill provides for.

2D) Valuable beyond security:
Supply Chain Efficiency was actually pioneered in the 1940's in post-World War II Japan by Edwards Deming in his transformative work at Toyota. He did this to drive up quality and profits. Automotive Safety pushes from the likes of Ralph Nader came 30 years later and were made much easier and less painful where these practices were applied. Deming pushed three supply chain management

principles:

1) Use fewer and better suppliers
2) Use the highest quality parts from those suppliers
3) Track which parts went where, so when something is defective, you can have a targeted, prompt, and agile response.

Some of the benefits of these three included:

1) Reduced production cost
2) Reduced product complexity
3) Reduced unplanned, unscheduled re-work
4) Reduced time-to-market
5) Reduced relationship management
6) Higher quality products
7) Fewer incidents
8) Faster mean-time-to-identify and mean-time-to-repair incidents
9) Happier customers
10) Etc.

Most of the projects I assisted with the private sector were driven by senior development leadership to drive developer productivity – or CIOs to drive more uptime, availability, fewer break-fixes, and faster mean-time-to-recover. These projects just also had the "collateral benefit" of massively reducing elective attack surface and risk.

There are other legal reasons to track software components, which are to remain in compliance with the thousands of licenses and terms applied to these open source projects. When I assisted with Mergers & Acquisitions for IBM (and elsewhere) legal/license risk was a key factor in our assessment of acquisition targets – and in competent selection for our development – to avoid lawsuits or obligations. In fact, many licenses require that you publically disclose use of their components. Dissenters are trying to avoid this, and some dissenters are doing so in violation of existing licensing.

I hope that my QFR answers were useful. I would be happy to go further if required.

Questions for Mr. Ray O'Farrell
Chief Technology Officer
VMware

Questions for the Record submitted by Chairman Will Hurd
Subcommittee on Information Technology
Committee on Oversight and Government Reform

(1) Mr. Corman (the witness from the Atlantic Council) called for a "software bill of materials" in his testimony to empower agencies to – be better informed in the procurement process, aid in evaluating a new vulnerability's effect and awareness of when product support expires. Please share your thoughts on feasibility, effectiveness and challenges with this idea.

Answer: The notion of a "software bill of materials" is potentially useful, but does not address all the challenges of the situation. Knowledge of the version of IoT software components and their provenance could be expected to be included in a "software bill of materials." The vulnerabilities identified in these components could lead to an assessment of the security of the device, however this is not adequate if taken alone. Specifically, the following issues make a "software bill of materials" an incomplete solution:

- IoT devices are low power and often highly constrained in their compute resources, and thus it is unlikely that they will be able to defend against any malicious attack and be completely self-reliant in establishing or sustaining an ongoing security posture.
- IoT devices may have very long intended life spans, and thus knowledge of security vulnerabilities at the time of manufacture are unlikely to be sufficient in protecting the device over its lifetime.
- IoT devices may well make use of software from open source and other communities, and thus may have supply chains from many contributing branches, making the provenance of all of the software difficult to determine.

Considering these points, effective protection of IoT resilience will rely on the capabilities of IoT devices as part of a broader IoT system, operating over a distributed IoT hosting platform and sustaining an ongoing security posture over the life of the device. The role of the platform will include the use of IoT gateways between the IoT device and the network. This will provide a trustworthy portal for enforcing industry best practices, assessing security posture, providing resilient protection and real-time analytics - even when network connectivity is lost.

In short, effective IoT device security is fundamentally a systems challenge, most effectively addressed in the context of the broader IoT platform. IoT security cannot be effectively addressed at the IoT device level.

(2) In the immediate term, what are some steps that agencies could, or should, be taking now to educate within and promote basic cyber hygiene practices in relation to the Internet of Things? What should we be looking at in addition to end point devices?

Answer: In the immediate term, I would suggest the following:

- Agencies should consider and assess the capabilities of IoT devices, and more importantly, the ability of any IoT systems' being considered for purchase to support the basic NIST security guidelines.
- Procurement of IoT devices is often done in the context of a process or operational task, for example, implementing a security surveillance system. The procurement team should be augmented with security professionals who have expertise in broad IoT and even data-center security. More and more, it is likely that the challenges faced in securing privacy within the data center will be needed to secure IoT and Edge devices.

With regards to endpoint devices, I think that, while applying cyber security principles to the end device is highly important, one should also focus the leverage of IoT gateways, network segmentation or other technologies capable of easily isolating parts of the IoT network if device compromise is suspected.

Establishing IoT behavioral visibility, policy-based control and real-time analytics at the gateway, at the edge and in the service hosting cloud/data center are essential aspects of realizing and sustaining trustable IoT operation.

(3) How would you envision IoT devices to comply with the NIST database that contains over 90,000 vulnerabilities and growing day-by-day?

Answer: The NIST database typically describes vulnerabilities and potential exploits of specific versions of software. Being able to associate a newly discovered vulnerability to a version of software within the device helps to alert us to potential exploits. The challenge here is to react quickly to the information in the NIST database. Understanding if the software in the device is affected by this vulnerability requires an ongoing security scanning of that configuration and the ability to update and address software that is known to be flawed. This requires a trustworthy platform to conduct this security management, one which is separate from the device, and one which is not being undermined if the device is compromised.

The gateway, edge, and service hosting platforms provide policy and assessment that will be reliable even when the IoT device is compromised.