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 PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro, and Workday.

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/.

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

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**

- 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.

more >>

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.