ITI

IT Alliance for Public Sector
A Division of ITI

July 28, 2017

Evelyn L. Remaley
Deputy Associate Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725,
Washington, DC 20230

Via e-mail to: *counter_botnet_RFC@ntia.doc.gov*

RE: ITI /ITAPS Comments in Response to NTIA's Request for Public Comment - "Promoting Stakeholder Action Against Botnets and Other Automated Threats"
(Docket No. 170602536–7536–01; RIN 0660–XC035)

Dear Ms. Remaley:

The Information Technology Industry Council (ITI) and the IT Alliance for Public Sector (ITAPS) appreciate the opportunity to respond to the National Telecommunications and Information Administration's (NTIA) Request for Public Comments (RFC), "Promoting Stakeholder Action Against Botnets and Other Automated Threats," noticed on June 13, 2017. We commend NTIA and the Administration for prioritizing a transparent and multi-stakeholder approach to tackling this critical issue.

ITI is the global voice of the tech sector. We are the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and this year we are pleased to be commemorating our centennial. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, Internet companies, and companies using technology to fundamentally evolve their businesses. ITAPS, a division of ITI, is an alliance of leading technology companies building and integrating the latest innovative technologies for the public-sector market. With a focus on the federal, state, and local levels of government, as well as on educational institutions, ITAPS advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Cybersecurity and cybersecurity technology are critical to ITI members. Facilitating the protection of our customers (including governments, businesses, and consumers), securing and protecting the privacy of our customers' and individuals' data, and making our intellectual property, technology, and innovation available to our customers to enable them to improve their businesses are core drivers for our companies. Consequently, ITI has been a leading voice in advocating effective approaches to cybersecurity, both domestically and globally.

Cybersecurity is rightly a priority for governments and our industry, and we share a common goal of improving cybersecurity. Further, our members are global companies, doing business in countries around the world. Most service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries around the world, servicing customers that typically span the full range of global industry sectors, such as banking and energy. We thus acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with – and drive – global norms, as well as the potential impacts on our customers. As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. In the technology industry, as well as banking, energy and other global sectors, when discussing any cybersecurity policy, it is important to consider our connectedness, which is truly global and borderless.

A central element of ITI's global advocacy efforts involves helping governments understand the critical importance of cross-border data flows to the ICT sector and the global economy, and the centrality of data to many cutting-edge technologies and innovations, such as the Internet of Things (IoT), Artificial Intelligence (AI) and big data analytics. Virtually every business that operates internationally relies instinctively on the free and near instantaneous movement of data across borders to enable their day-to-day business operations, from conducting research and development, to designing and manufacturing goods, to marketing and distributing products and services to their customers, to securing global networks and the personal data of customers across the globe. With data increasingly at the center of not only the global economy but our lives, securing that data, and protecting privacy of that data, is of paramount importance to ITI's companies, and the data-driven innovations mentioned above are increasingly critical to our shared cybersecurity mission. In addition, U.S. and global ICT companies have a long history of exchanging security-related information across borders with geographically-dispersed employees, users, customers, governments, and other stakeholders, which helps them protect their own systems and maintain high levels of security for the technology ecosystem. We urge NTIA to bear in mind the critical importance of global data flows to continued economic development, Internet growth, and of course, cybersecurity as it evaluates the feedback it receives in response to this RFC and crafts its recommendations.

ITI has not endeavored to answer all the questions posed by NTIA in the RFC, but instead focuses our comments on the key issues that we believe will prove most helpful to NTIA in addressing this complex and important topic. We organize our discussion of these issues under the overarching question headings identified by NTIA.

WHAT WORKS: Identifying Successful Policy Approaches

ITI, as a global trade association, is well-situated to provide comments on broader policy approaches that have proven successful in helping to improve our collective cybersecurity posture, rather than identifying specific technical approaches to addressing botnets and similar threats (though we are sure many of our members will individually provide more technical comments). Below we identify several broader policy approaches that we advocate for in the context of both addressing botnets and other automated distributed attacks, and cybersecurity more broadly.

Prioritize Risk Management-Based Solutions and Avoid Prescriptive Regulatory Responses

Cyberattacks, including botnets and other automated distributed attacks, can never be entirely prevented. Security is a continuous process of risk management, technology development, and process improvement that must evolve with today's highly complex and dynamic computing environment. Thus, prescriptive regulatory or legislative solutions are unlikely to provide a lasting solution to cybersecurity concerns, as they can quickly become outdated as technology changes. Government must give the market an opportunity to address the shortfall in IoT security; however, if security does not improve the government should examine what levers it can pull to shift the market in a way that drives security but does not impact innovation, particularly with regard to critical infrastructure. The IoT, for example, includes both modern and legacy elements. Legacy features are frequently targeted by attackers. The 2016 Mirai botnet attack targeted many older devices that do not use modern, standard industry best practices for cybersecurity. As products constantly change, and new threat scenarios emerge such as the IoT, this underscores the need for nimble risk management-based approaches. At the 2016 Chamber of Commerce Cybersecurity Summit, U.S. Secretary of Commerce Penny Pritzker stated, "no static checklist, no agency rule, no reactive regulation is capable of thwarting a threat we cannot foresee."[1] As it continued to study the issue in its 2017 IoT green paper, the Department of Commerce noted, "overly prescriptive regulations could impede stakeholders' abilities to respond to ever-changing threats…."[2] This guidance is applicable broadly, as well as to botnets and automated threats that may exploit weaknesses in substandard legacy or even new devices connected to the IoT. We recommend the federal government seek flexible, risk management solutions that are adaptable in multiple industries rather than mandate prescriptive checklists that slow, or even halt, security innovation.

Leverage the NIST Framework's Consensus Standards and Public-Private Partnership Based Approach

Cybersecurity is based on a dynamic process of managing risk and assessing best practices. Effective approaches to cybersecurity are grounded in sound risk management principles and demand a greater emphasis on consensus driven industry, international, standards-based approaches, such as the principles embodied in the National Institute of Standards & Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity ("Framework").[3] The Framework and other public-private cyber cooperative practices enable greater collaboration to protect networks and stay one step ahead of hackers and cyber criminals.

The Framework should serve as a reference point for the Administration as it seeks to counter the proliferation of botnets and other automated and distributed attacks. We believe the Framework has already helped and will continue to help improve cybersecurity of critical infrastructure entities and beyond, and we remain committed to helping it succeed amongst a broader array of stakeholders. From our perspective, the Framework has had and continues to have an important, valuable impact on organizations' understanding of cyber risks. The Framework has allowed organizations to have useful conversations about cybersecurity risk management both internally (e.g. with our senior management) and externally (e.g. with boards of directors, partners, suppliers, and customers), allowing these parties to better understand the importance of managing cyber risks, including botnets and automated threats. The Framework's common terminology (identify, prevent, detect, respond, recover) provides a flexible,

[1] U.S. Chamber of Commerce, Fifth Annual Cybersecurity Summit, *Enhancing Businesses' Cybersecurity Awareness and Protecting America's Digital Infrastructure*, Penny Pritzker, Secretary, U.S. Department of Commerce, September 27, 2016, *available at* https://www.uschamber.com/event/5th-annual-cybersecurity-summit.

[2] Department of Commerce, Internet Policy Task Force & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things,* January 2017, at 25, *available at* https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

[3] *See Framework for Improving Critical Infrastructure Cybersecurity,* February 12, 2014, available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

common, standardized language to enable these discussions. To further expand the Framework's impact to better protect critical infrastructure as well as all organizations, we recommend the following:

Leverage the Framework's Mapping to International Standards. The Framework's mapping to international standards such as ISO/IEC 27001 is helpful, as such standards help organizations establish an immediate linkage between their ongoing risk management and certification efforts. This type of mapping provides an extremely persuasive example to share with governments outside of the United States that may be considering their own national cybersecurity frameworks/initiatives. By mapping the Framework's security guidance to global standards, the Framework demonstrates that national cybersecurity concerns can be addressed in a manner that bolsters global standards. Getting standards in place – for instance, regarding automated patching - is essential to managing increasingly complex and evolving risks, such as those associated with botnets.

Expand use of the Framework by Suppliers. In recognition of the importance of addressing global supply chain security concerns, some companies have begun exploring how to expand Framework use with their suppliers. Two types of instances in which owners and operators of critical infrastructure (CI) services should consider requiring use of the Framework across their supply chains are: (1) where an owner/operator has outsourced the management of any part of its operation via a managed services partnership; and (2) where the supplier is considered a critical business partner, such that any disruption of their business would affect the delivery of critical services. Companies can also take proactive steps to encourage use of the Framework across by their ecosystem partners by, for example, integrating the Framework into their supplier guidelines. Having effective standards in place is only half the battle – once we do, larger more established companies can play a significant role in propagating their use across their supplier ecosystems and beyond.

Develop Implementation Guidance for SMBs, Including New Market Entrants and Startups. Not all companies have mature programs or the technical expertise to keep up with the latest developments in cybersecurity – such as the Framework – to appropriately manage cyber risk. SMBs have reported being confused and even overwhelmed by the size and complexity of the current Framework, and with respect to newer innovations such as IoT, many startups and new market entrants may lack the resources or know-how to digest and apply the Framework without some assistance. Given the interconnected nature of the cyber ecosystem, we are keenly aware that cyber elements of the critical infrastructure can be compromised by weaknesses in smaller entities to which they are technologically connected. Given this fact, it is critical for us to create a sustainably secure cyber ecosystem for all entities, large and small. Therefore, as the Framework continues to evolve, we recommend that interagency partners work together, including NTIA, NIST, the Department of Homeland Security (DHS), the Small Business Administration, and Sector Specific Agencies, to better understand the cybersecurity and implementation challenges faced by organizations of all sizes, and consider ways to make the Framework more approachable for all organizations. The USG should prioritize understanding the issues confronting theses smaller entities and addressing their unique concerns and needs.

Encourage Regulatory Streamlining by Promoting Framework Use by Regulators Domestically. ITI has previously advocated that the Framework can be used to drive cybersecurity alignment across federal agencies, so we were pleased that the Trump Administration's recent cybersecurity Executive Order requires federal agencies to use the Cybersecurity Framework. Alignment of federal agency cybersecurity practices, including orientation of federal agency efforts to the Framework, will help facilitate mapping of agencies' cybersecurity risks to their missions government-wide. Further still, adoption of consensus industry best practices by large federal government consumers of information technology will help consensus best practices and standards gain broader traction in the marketplace. The Administration should consider developing guidance for federal agencies applying the NIST Framework to help them use business drivers to guide cybersecurity activities and consider cybersecurity risks as part of their risk management processes. In other words, the USG should develop government-wide recommendations as government "sector-specific guidance" in the manner in which many other sectors (such as the financial and energy sectors) currently are developing for themselves. Perhaps more importantly, any regulatory efforts by those same agencies should be streamlined to reduce regulatory redundancy – providing Administration guidance aimed at orienting any such efforts toward the Framework is the surest way to accomplish this.

We believe more can and should be done to reinforce the Framework as voluntary, while at the same time embracing its sensible use by regulators to streamline and on a net basis reduce cybersecurity regulations. How can we accomplish this? The key is that the Framework should not serve as the impetus or rationale for extra layers of regulation – that's not regulatory streamlining, it's regulatory redundancy, and multiple layers of redundant regulations will not create better cybersecurity for anyone, including regulated entities themselves. Rather, the Framework can still be held up as a voluntary risk-management based tool, while also serving as a beacon around which policymakers at every level – including regulators – should orient their efforts to improve cybersecurity. Doing so in turn will help reduce regulatory redundancy.

Further International Cybersecurity Framework Alignment Efforts. Driving international Framework alignment can help accelerate adoption of critical cybersecurity standards, and foundational to driving such alignment involves the global Framework promotion efforts of both industry and government. As a sector, we have supported organizations across the globe who are using the Framework as the basis to assess their actual cybersecurity risks. The Framework is gaining traction internationally, and familiarity is growing in multiple geographies (e.g., Italy developed its own version of the *Framework* using a similar public-private partnership process Israel has incorporated the Framework into its own cybersecurity guidance, and the British Standards Institute is developing a standard that assesses organizations' application of the *Framework)*. NIST has collaborated on these efforts, and has additionally engaged with approximately thirty interested governments globally on Framework education, outreach and development efforts. Further, international use of the Framework is gaining support across several critical sectors, including Financial, Electric Utilities, Water Utilities and Oil and Gas, and is being used to establish security requirements and as a way to recommend threat mitigation controls and remediation. Promoting the Framework will help the US to sustain its leadership on cybersecurity around the world, and this will in turn help to further enhance the Framework's use within the United States.

To facilitate further global adoption, Federal agency partners should promote the Framework approach with their global government partners. For example, the Department of State should reference the Framework in its global cybersecurity capacity-building efforts, and feature the Framework in the International Cybersecurity Strategy under development pursuant to the Trump Administration's cybersecurity executive order. Likewise, the White House should highlight the Framework in its strategic cybersecurity partnerships. International acceptance of industry-led, global cybersecurity standards will help drive even greater competition and innovation in the global marketplace.

The USG should also consider other mechanisms by which to expand the Framework approach. For example, given the increasing global acceptance of the Framework, we would support NIST exploring, with industry stakeholders, the opportunity for submitting the Framework as an international standard. This could be a valuable contribution to further harmonizing cybersecurity practices on a global scale. Today more than 80 countries are in the process of creating new cybersecurity regulations and there are myriad implementing requirements being considered. Adding the Framework as an international standard could help propagate globally the standards based approach needed to meet the challenges raised by botnets and other automated distributed threats.

<u>Focus Policies on Security by Design, not Geography, and Promote Secure Development Practices.</u>

The global digital infrastructure and Internet ecosystem includes a range of technologies and products. Many leading technology companies employ secure development lifecycles and security by design techniques (incorporating security throughout the product development phase), and some participate in global, industry-led efforts such as SAFECode to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services.[4] Security is defined by the process used to make a product, not the location of the manufacturer—a function of how a product is made, not where a product is made. There are several ways to better secure the IoT ecosystem, including the adoption of edge systems like IoT gateways, that secure manageable infrastructure through the complete lifetime of IoT devices. ITI companies invest heavily in security because their business's reputation depends on protecting consumers and earning their trust.

Leading technology companies integrate security into their products – stakeholders should collaborate to promote the uptake of such practices more broadly. ITI's member companies are at the forefront of providing security solutions from the devices at the expanding network edge to the cloud, and across the network and IoT. With billions of additional devices coming online, ITI's companies ensure that security is embedded in Internet platforms including IoT from the beginning of the manufacturing and design process for each new device that extends and expands the network. Security must be built into both hardware and software at the outset to ensure there are redundancies, to prevent intrusions, and to create secure and trusted IoT systems. Advances in hardware-based security make security features stronger. For example, semiconductor manufacturers can design processor chips with built-in safeguards. Support for encryption and key management can now be incorporated in hardware, such as semiconductors, providing protection against a greater number of attacks. Manufacturers can also prevent chips from being modified by designing fuses into chips. If a hacker attempts to access or rewrite the data, the fuse pops and prevents the unauthorized modification. It is also possible to package security technology into different components to harden and secure hardware, software, and communications to assist developers in building secure and efficient IoT applications from the ground up. In addition, a semiconductor manufacturer can use EPID (Enhanced Privacy Identification) technology, which is an industry standard used for data privacy, in the device processors so an IoT system can trust that the data it is using is coming from a known and secure device.

One of the most effective ways in taking action against botnets and other automated threats is to prevent them from taking hold in the first place. Once they have a footprint and have established themselves, they are difficult (maybe impossible) to remove or remediate. While there are no silver

[4] For more information on SAFECode, see https://www.safecode.org/.

bullets in preventing such an attack, and even the best designed devices can fall prey to new attack methods or vectors not envisioned during a product's design, resiliency mechanisms can be used to strongly mitigate the likelihood of persistent infection. Resiliency in devices has recently been articulated in a draft of NIST Special Publication 800-193. Device manufacturers employing the articulated principles of protection, detection and recovery to provide resiliency in the devices themselves will be best positioned to mitigate against these attacks.

Similarly, on the network side, devices communicating with the network will require a reliable level of service and connectivity, as well as high security to prevent unwanted intervention. New Internet protocol architectures are more adaptable and use advanced technologies to pervasively distribute security, treat individual users and devices with an appropriate level of performance and privacy based on their needs, and automate manual processes to improve scale and availability. Application programming interfaces (APIs) facilitate data interactions between edge devices, code modules, applications and backend IT systems. Organizations can leverage API management software to address security as an architectural challenge in the development of IoT applications.

Another useful technology gives organizations the ability to scan the network to discover connected devices, enabling them to have visibility of all devices and other "things" connected to their networks. One company has developed a security tool which automatically discovers all Internet Protocol (IP) or IP-enabled devices, including IoT devices, that are connected to the network. Data collected from traversing the network is collected and analyzed for odd behavior, and anomalous devices are either removed from the network or quarantined. For example, if a home automation device attempts to communicate with a financial services server, it could indicate a breach. When that kind of suspicious network traffic is discovered, the security tool can disconnect the device from the network, minimizing the damage. Other companies provide software that authenticates communications between devices, applications and back-end systems, using credentials or other unique identifiers; if the software suspects a device is compromised or detects malicious activity, it can close these interfaces.

Many IoT devices operate in machine-to-machine mode, without direct user interactions. Simple upgrades to such devices can increase security, as well as mandating password changes or requiring a full set up for security and privacy features prior to use. Many IoT devices are delivered with default user information and passwords. While users can and should change those credentials before operating such devices, they often do not—thus creating a potential vulnerability for would-be attackers to exploit. To avoid this risk, a company can deliver devices that prompt for a mandated password change upon first use. In addition, some devices leave it to the user to improve security by leaving access controls turned off. Instead, a company may enable security options by default or as part of an initial setup process so that users must consciously decide to remove the default protections rather than the opposite—in effect forcing users to improve security on their own.

NTIA's recent convening of a public-private sector working group and running of a multi-stakeholder process to address IoT security upgradability also bears noting in the "what's working" category. While we won't belabor the details of a multistakeholder process with which NTIA is intimately familiar, it is worth highlighting the process as another example of leveraging a public-private process to address cybersecurity challenges, as well as the versatility of such processes to tackle diverse aspects of cybersecurity, including technical capabilities, existing standards and tools, communicating best practices, and incentives and barriers to adoption. We discuss this NTIA effort further in the "Gaps" section below, particularly the one working group that has completed its work ("Communicating Upgradability and Improving Transparency").

GAPS: Identifying Areas for Improvement

Connecting equipment is a long-term commitment – not a one-time design and manufacturing cost. Creating and delivering "smart," connected, and enhanced equipment requires attention to the care and handling of that equipment over the full life-cycle of its in-service lifespan. Equipment that can and will support connectivity to networks and communications to and from it will require software and firmware updates from time to time, if only to prevent or defend against attacks that were not ever known at the time of original manufacture. Just as physical equipment requires periodic maintenance and attention, the software running within equipment will require ongoing attention and maintenance. Such considerations must be evaluated when building, deploying and using such equipment by all entities, whether large or small, or established market players or new entrants. Unfortunately, best practices are not necessarily adopted or employed by new device manufacturers in the IoT space, leading to gaps which can be exploited by adversaries seeking to propagate botnets or other attacks. We describe a few of these gaps, long with proposals to help close them, below.

Smaller and Newer Market Entrants Beget Uncoordinated, Immature Approaches

One such gap is created by the significant number of startups and other new entrants seeking to leverage IoT and other innovative extensions of the Internet. Many of these smaller and newer developers are not using best practices identified in the previous section, such as secure development practices. Finding ways to effectively spread awareness of such practices is key. A related problem or gap is that the diversity of newer and smaller entrants leveraging IoT and other innovations are not developing integrated approaches that work across disparate networks that were heretofore unconnected. It is clear we need a more integrated approach to development that pulls in a diversity of market participants. Another related issue that may indeed be holding some smaller, newer ecosystem players back from adopting best-in-breed cybersecurity practices and standards (such as those identified in the Framework) is cost. We thus need to figure out how to make development practices more scalable and cost-effective.

How can we address these gaps? First, it bears repeating that both industry and government have roles to play. A promising effort that should be embraced is NTIA's recent public-private partnership work on IoT security upgradability, referenced above. One of the NTIA IoT working groups convened as part of its multistakeholder process has already completed its work – the "Communicating Upgradability and Improving Transparency Working Group." While this work focused on just a piece of a larger problem regarding IoT upgradability, the progress made there is instructive and provides a useful template for making progress on something that is arguably exacerbating the larger botnet problem. The working group posited that security updates are a key way to protect IoT devices when vulnerabilities are discovered and attacks evolve, though the method and capability of IoT devices to receive security updates varies across devices, services, and deployments, and that consumers of IoT devices may desire basic information about their devices' security capabilities, particularly with regard to whether and how devices receive security updates.

The working group developed guidance that is not prescriptive, but rather suggests categories of information about updatability that IoT device manufacturers might consider communicating to users, including key elements such as describing whether IoT devices can receive security updates. While not definitive, this is the type of foundational work and approach that can be built on to address other dimensions of the cybersecurity challenge as we know it today, including botnets and other automated and distributed threats.

From the ITI perspective, we are actively working with our member companies to tackle this very issue of better coordinating and communicating our "security accountability" – including our own secure development practices and our leading work on developing security standards – to consumers and policymakers. We understand that we, and other industry sectors, have a role to play in trying to develop and promulgate such standards and practices across the Internet ecosystem, particularly to new entrants and other smaller, less-resourced, newer market participants in dynamic segments such as IoT. While we don't yet have all the answers in this regard, we want to continue to work with NTIA and other stakeholders to figure out how we can engage constructively, and as mentioned above are also looking at what we can do to impact our corner of the Internet ecosystem, such as integrating cybersecurity standards such as those embodied in the Cybersecurity Framework into our supplier guidance and contracts.

Cross-Border Data Flows, Siloed Policy Approaches, and Cybersecurity

We commend NTIA for calling out the international dimension of the botnets and automated threats problem, in acknowledgement of the global nature of our cybersecurity challenges, and the centrality of cross-border data flows to the modern digital economy.

A central element of ITI's global advocacy efforts involves helping governments understand the critical importance of cross-border data flows, not only to the ICT sector, but also to the global economy. Virtually every business that operates internationally relies instinctively on the free and near instantaneous movement of data across borders to enable their day-to-day business operations, from conducting research and development, to designing and manufacturing goods, to marketing and distributing products and services to their customers. U.S. and global ICT companies also have a long history of exchanging security-related information across borders with geographically-dispersed employees, users, customers, governments, and other stakeholders, which helps them better protect their own systems and maintain high levels of security for customer data, IP and the technology ecosystem.

Indeed, as well as facilitating secure business transactions amongst companies in disparate locales, global data flows are key to greater coordination and productivity for global companies, helping to secure the systems and networks that manage production schedules and Human Resource (HR) data, as well as communicate internally with subsidiaries and employees in different geographies. The free flow of data across borders is also necessary to enable a seamless and secure Internet experience for hundreds of millions of citizens around the globe. Unfortunately, we can point to several examples of a troubling global trend of erecting barriers to the free movement of global data, both in the U.S. and abroad – for instance, Wassenaar Export controls related to intrusion detection software, the 2015 European court of Justice opinion invalidating the Safe Harbor transatlantic data transfer agreement, and forced localization measures in numerous countries.

Perhaps even more disturbing, the trend of impeding data flows generally is contrary to the thrust of current U.S., and indeed global, cybersecurity policy, and threatens to undermine continued global cybersecurity progress.

To illustrate, it is well known that in recent years U.S. policy has prioritized advancing cyber threat information sharing, and in 2015, Congress passed a bipartisan cybersecurity threat information sharing bill, the Cybersecurity Act of 2015.[5] The bill acknowledges that voluntary sharing of information regarding cyber threats, with appropriate privacy safeguards, is an integral component of improving our cybersecurity ecosystem, as it helps all stakeholders better protect and defend cyberspace. More specifically, CISA required the heads of various federal security agencies to jointly develop procedures to ensure the Federal Government maintains "a real-time sharing capability," and further required the Department of Homeland Security, in coordination with industry and other stakeholders, to develop an automated capability for the timely sharing of cyber threat indicators and defensive measures. Clearly, both cross-border data flows and real-time information sharing is essential in combatting security threats to the global ICT environment, including botnets and automated threats. These policy efforts are intended to spur the voluntary sharing of cyber threat information among and between businesses and government entities to improve cybersecurity, and these initiatives contemplate the sharing of cybersecurity threat information as inclusive of information related to vulnerabilities.

Given that the overarching intention of these policy initiatives is to promote expedited sharing of threat information to improve cybersecurity, we are concerned that the2013 additions to the Wassenaar Arrangement, if implemented, could undermine this key principle and severely complicate the ability of companies in all sectors and government entities to share information in real-time to protect and enhance their security. Implementation of the Wassenaar controls would necessarily slow down the sharing of vulnerability information (both intra-company and between companies). In other words, because the Wassenaar controls are effectively erecting additional barriers to vulnerability sharing, it appears diametrically opposed to the goals of multiple cybersecurity policy initiatives recently advanced by U.S. government policymakers. While the USG and other stakeholders continue to advocate for fundamental changes to the Wassenaar arrangement to fully address the problems recapped above, we believe recounting our collective experience with the problematic Wassenaar cybersecurity export controls helps to illustrate how policies that impede data flows can also undermine cybersecurity, inclusive of efforts to counteract botnets.

Ways in which policymakers can help close some of these gaps include:

Encourage the use of high-level cybersecurity best practices, particularly for small businesses and consumers. Congress and certain federal agencies can encourage the use of high-level cybersecurity best practices that incentivize good cyber behavior. For example, the Small Business Administration (SBA) has established programs to educate small and medium-sized business owners (SMBs) about cybersecurity, provide resources to assess information security resilience, and create customized cybersecurity plans. Congress can reinforce these and other existing programs by providing more resources for agencies to educate SMBs on risk management and promote the use of processes and procedures to protect information systems against cybersecurity threats. Thus, SMBs will not only implement better cybersecurity practices, but also contribute to more secure supply chains for large

[5] Consolidated Appropriations Act, 2016, H.R. 2029, 114th Cong., Division N (2015).

businesses and the federal government. Similarly, the FTC continuously provides and updates information for consumers to improve their online security practices, and information on securing connected devices in the IoT. The USG could also consider directing the SBA to work with NIST and Small Business Development Centers (SBDCs) to address IoT security by creating, maintaining, updating, and disseminating cybersecurity resources specific to SMBs development, adoption, and use of IoT products.

Avoid geography-specific or siloed, sector-specific regulatory approaches, as doing so will help improve cybersecurity and nurture IoT development. As stated above, security is defined by the process used to make a product, not the location of the manufacturer—a function of how a product is made, not where a product is made. Federal cybersecurity policies should thus avoid using geography as a proxy for product security. Similarly, it is counterproductive to create siloed approaches to cybersecurity across diverse information technology (IT) applications simply because they are helping to connect more "things" to the internet in an increasingly interconnected world. Indeed, to fully realize the benefits offered by the IoT, the federal government should promote policies that help break down barriers to connecting devices and correlating data. Government bodies seeking to address IoT security must look at the underlying technologies and assess where current authority, oversight, and regulation already exist; should seek to leverage the cybersecurity expertise of agencies such as the Department of Homeland Security; and replicate areas where government approaches are working. The alternative – a world in which we endeavor to separately regulate each new IT application or IoT industry segment– is not realistically scalable, and simply unsustainable in the IoT world.

GOVERNANCE AND COLLABORATION

Industry and the Federal Government should continuously invest in collaborative responses and processes. The tech industry constantly works to stay ahead of threats, not only through its own solutions but also in partnership with the federal government. The IT industry leads and contributes to a range of significant public-private partnerships, including information sharing, analysis, and emergency response with governments and industry peers. Some examples include:

- NIST Cyber-Physical Systems Working Group on security and privacy;
- NIST Framework for Improving Critical Infrastructure Cybersecurity;
- NIST Cybersecurity for IoT program;
- National Telecommunications & Information Administration (NTIA) Multi-stakeholder process on IoT patching;
- Department of Homeland Security (DHS) IoT security principles;
- Federal Trade Commission (FTC) 2015 Internet of Things Staff Report;
- Department of Defense (DOD)-Defense Industrial Base (DIB) Cybersecurity (CS) Information Sharing Program;
- Information Technology Information Sharing and Analysis Center (IT-ISAC); and
- Sector Coordinating Councils (SCCs).

Most if not all other U.S. industry sectors make significant contributions to cybersecurity public-private partnerships and could compile similar lists. As convergence continues and we continue to connect more networked "things" together, we are reminded that we need a full complement of these diverse stakeholders collaborating and working together – both with each other, and with our government counterparts. Even within the tech sector and ITI's membership specifically, we have a diversity of players – for instance device manufacturers, software developers, and cloud providers – but also auto manufacturers and others who all have roles to play in this debate. When we pile on all the other sectors of the U.S. economy, including startups and other new entrants, that means we will potentially need a lot of seats at the table – but the nature of autonomous and distributed attacks and similarly complex problems in the age of an Internet of Everything demands that we invite as many potential participants as possible. Policymakers and regulators should reinforce this collaborative environment to encourage innovative, private-public cooperation on these issues, rather than top-down regulations that may duplicate ongoing work. Through oversight, policymakers should also better coordinate the many IoT security related policy efforts currently in progress across the administration.

POLICY AND THE ROLE OF GOVERNMENT

Take Stock of Existing Authorities Before Creating New Ones. The rapid growth of networked devices and Internet applications due to the availability of components, Internet service, and the technology that make Internet connection possible – whether we are talking about Smart Grid, Smart Cities, Connected Autos – have us fast headed toward an Internet of Everything. Given this, USG and other government bodies must look at the underlying technologies and assess where current authority, oversight, and regulation already exist. It should also seek to identify areas where government is approaching this correctly, and replicate that activity in other areas. There are many relevant policy areas where authorities already exist, where government is facilitating IoT development, and where industry is working with government to address new or evolving issues stemming from the IoT, including cybersecurity and related issues. Two recent stock-taking efforts worth noting include DHS' recent undertaking to survey and compile existing and uncoordinated efforts across the federal government to address IoT security, and NTIA's IoT upgradability working group assessment of existing IoT security standards. It will be important to build on this work to drive more coordinated federal activities in this space to ensure that stakeholders are not operating at cross-purposes.

USG's Role as Convener. Significant activity continues to take place across both government agencies and the private sector in an effort to strengthen our cybersecurity, including for IoT. The interests of government agencies and industry are aligned in this arena in that both aim to minimize vulnerabilities and create networks, products, and devices that are as secure as possible. Consequently, much of the activity designed to enhance cybersecurity takes place in consultation and close collaboration with the private sector, and we strongly encourage that public-private partnership (PPP) approach to continue.

USG stakeholders have a critical role to play in fostering security across the Internet ecosystem; excellent groundwork has already been laid in this area and should be leveraged going forward. The tech sector has been partnering with the NIST for nearly three years developing and using the Framework, discussed at length earlier. It is instructive to recall the genesis of the Framework stems from Executive Order 13636,[6] issued in February 2013, which called for the government to partner with owners and operators of critical infrastructure to improve cybersecurity through the development and implementation of risk-based standards. Development occurred through a process of coordination and collaboration convened by NIST between the technology industry, others in private industry, and U.S. government partners. What resulted is a set of voluntary guidelines, best practices, and standards to

[6] *See* White House, Executive Order 13636, Improving Critical Infrastructure Cyber Security, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

help critical infrastructure, businesses, and other private and public actors to better manage cybersecurity risks. Taking a similar public-private partnership approach, NIST subsequently released a Framework for Cyber-Physical Systems[7] (the "CPS Framework"), also developed in partnership with industry, academic, and government experts. One of the key working groups in the cyber-physical systems project focused on cybersecurity and privacy.[8]

ITI believes it is pivotal to continue to replicate this partnership approach in addressing modern cybersecurity challenges, whether we are tackling IoT security or threats such as botnets

INTERNATIONAL: A Global Problem Demands Global Solutions

Driving Global Cybersecurity Standards Together. The global ICT industry is heavily invested in developing standards to address important challenges in security management. We urge the USG to continue taking a leadership role in promoting the adoption of industry-led, voluntary, globally recognized cybersecurity standards and best practices, to make the preservation and promotion of a global market a primary goal in any product assurance requirements, and avoid country-specific requirements. We also welcome and encourage all governments to participate in standards development activities, particularly in private fora and consortia. Governments might also consider greater action in their own (public sector) use of voluntary, globally accepted standards or generally accepted industry practices for cybersecurity risk management. Indeed, government leadership can demonstrate such standards' importance and may be necessary to overcome economic disincentives to adoption of standards that yield benefits to the network as a whole.

We applaud the USG for continuing to invest in global standards development (e.g., the NIST-led Interagency Report on Strategic U.S. Government Engagement in International Cybersecurity Standardization).[9] However, it's worth noting the purpose of furthering international cybersecurity standards is not for governments to turn around and mandate their adoption. From ITI's perspective, any effort to mandate minimum security standards is problematic, in that it is difficult for a minimum standards approach to allow for the flexibility for best security practices to evolve as technology advances, or to fully consider the necessary risk management practices at the heart of cybersecurity. ITI thus strongly cautions all governments not to set compulsory security standards for the commercial market– whether they are standards vendors must follow as they build their products or services, or standards that would guide consumers when purchasing ICT products and services or conducting business with companies. Such an approach could encourage some firms to invest only in meeting static standards or best practices that are outmoded before they can even be published or cause others to divert scarce resources away from areas requiring greater investment towards lower priority areas. To maintain (rather than restrain) innovation and to prevent the development of single points of failure, any standards should be purely indicative, their use entirely voluntary, and should always allow organizations to adopt alternative solutions. Defining new, country-centric standards has many downsides as such insular standards may conflict with global standards currently in use, interfering with global interoperability.

[7] *See* NIST CPS Draft Framework: http://www.cpspwg.org

[8] http://www.nist.gov/cps/cpswpg_security.cfm

[9] *See* NIST-IR 8074, Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf

Global standards, interoperability and IoT. Many of the existing foundational elements that drove the development, evolution, and investment in the internet ecosystem must be continued to fully realize the potential of Internet and data-driven innovations such as the IoT and AI. Adoption of global, voluntary standards is critical for supporting the interoperability necessary for the modern Internet ecosystem to thrive. Integrating multiple layers of security at the outset of a product's design phase enables more robust IoT deployments, and offering open standards makes security more widespread in the massively-connected IoT ecosystem.

As the IoT technology landscape comes into greater focus, various global, industry-led standards-setting organizations (SSOs) have formed technical and study groups to ascertain to what extent additional standards development is necessary, including for cybersecurity. These bodies are typically international in scope, drawing experts and participation from across the globe and across various industry sectors that will be impacted by and benefit from IoT. It is important for the Department of Commerce and, more generally, all governments to share their needs and requests with these SSOs and, when appropriate, to actively participate. Federal agencies should actively consult with industry regarding when and where to invest their time and resources in support of standardization efforts. The USG should strongly encourage governments to focus their time and resources on participation in and supporting industry-led standardization activities. When multilateral organizations are determined to proceed anyway, the USG should strongly encourage them to allow full industry participation, and to look to existing or pending global standards before undertaking any activity to engage in standardization activities that may be duplicative of, or even conflict with, global industry-led IoT standards.

The U.S. government should continue to encourage open and international security standards to maintain the long-term viability of the Internet and IoT and to foster solutions that are interoperable and reusable across a variety of use case deployments, vendors, sectors, and geographies. We support NIST's continued collaboration with international standards bodies as it addresses IoT security during its ongoing work. This includes collaboration on International Organization for Standardization (ISO) activity on security, privacy, cybersecurity, and IoT. Other organizations creating standards for IoT that could impact our collective efforts to mitigate threats from botnets include:

- **Industrial Internet Consortium (IIC)** – The IIC is a global, member supported organization that promotes the accelerated growth of the Industrial Internet of Things (IIoT) by coordinating ecosystem initiatives to securely connect, control and integrate assets and systems of assets with people, processes and data using common architectures, interoperability and open standards to deliver transformational business and societal outcomes across industries and public infrastructure.
- **Open Connectivity Foundation (OCF)** – The OCF is defining connectivity requirements to improve interoperability between the billions of devices making up the IoT. OCF will deliver a specification, an open source implementation and a certification program ensuring interoperability regardless of manufacturer, form factor, operating system, service provider or physical transport technology.
- **Open Fog Consortium** - Driving industry and academic leadership in fog computing architecture, testbed development, and a variety of interoperability and composability deliverables that seamlessly leverage cloud and edge architectures to enable end-to-end IoT scenarios.
- **IoT Security Foundation** – Driving investigation and leadership in securing IoT devices, concentrating on consumer equipment.

USERS: Driving Education and Awareness

We in large part focused our preceding comments on identifying and addressing gaps with respect to business and policymaker practices. With respect to users or consumers, some of the challenges we face in a world of proliferating internet-connected devices and increasing bandwidth are perhaps even more acute. One promising tack for addressing the consumer education and awareness problem that was perhaps an undercurrent of the NTIA work cited earlier around communicating upgradability and improving transparency is to prioritize solutions that take consumers out of the security equation (or at least, decreasing the consumer's burden to a manageable level), by focusing on IoT devices' capacity to be automatically updated. Just as our recent policy efforts have sought to automate cybersecurity threat information sharing, we need a policy effort oriented around promoting best practices for automating security updates, particularly for IoT products made by newer, smaller, less experienced market entrants. Of course, such an approach does place some responsibility on device manufacturers and others to figure out ways of communicating important information to users like the capacity of their devices to receive automatic updates (where appropriate). While there is still much work to be done to figure out the best mechanism for doing so, we believe that organizations' that wish to demonstrate their accountability will rise to the challenge.

Cyberspace's stakeholders - consumers, businesses, governments, and infrastructure owners and operators - need to know how to reduce risks to their property, reputations, and operations. However, as articulated above many stakeholders are not aware of and do not adequately utilize the range of tools available to them, such as information sharing, risk management models, technology, training, and globally accepted security standards, guidelines, and best practices. Raising awareness so that cyberspace's stakeholders can use these tools is critical to improving cybersecurity.

Another option on the consumer front is to direct the FTC to work with NIST to create, maintain, and update cybersecurity resources for consumer development, adoption, and use of IoT products. Consumer education programs should provide guidance to consumers to look critically at IoT devices they deploy directly in their home Wi-Fi networks. Such consumer guidance should also consider providing a series of questions for consumers to ask vendors (i.e. how do you deploy security fixes?) to limit any associated risks.

CONCLUSION

ITI would like to thank NTIA for demonstrating a commitment to utilizing transparent processes and partnering with the private sector to advance our shared cybersecurity goals. We would also like to commend the Administration for its willingness to engage with our companies and the ICT industry to determine how government and industry can best work together to address botnets and other automated and distributed threats, and to improve cybersecurity more broadly. The commitment to industry outreach is an excellent example of how effective public-private partnership processes can help to improve cybersecurity.

While we won't recap all our recommendations here, we will reiterate the importance of furthering risk-management and flexible approaches grounded in international standards that leverage public-private partnerships – all of which are hallmarks of the Cybersecurity Framework. We urge NTIA and the

Administration to leverage the Framework and hold up the Framework approach as a model that can help address the botnet problem and improve cybersecurity not only in the U.S., but globally.

ITI and our members look forward to continuing to work with NTIA and other stakeholders across the Administration on this and other initiatives to improve our cybersecurity posture. Please continue to consider ITI as a resource on cybersecurity issues moving forward, and do not hesitate to contact us with any questions regarding this submission.

Sincerely,

John Miller
Vice President for Global Policy and Law
Cybersecurity and Privacy