Information Technology
Industry Council

May 27, 2015

Allan Friedman
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave, NW
Room 4725
Attn: Cybersecurity RFC 2015
Washington, DC 20230

Via e-mail to: securityRFC2015@ntia.doc.gov

Attn: Cybersecurity RFC 2015, Request for Comment on Stakeholder Engagement on Cybersecurity in the Digital Ecosystem

Dear Mr. Friedman:

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to your RFC of March 19, 2015, "Request for Comment on Stakeholder Engagement on Cybersecurity in the Digital Ecosystem."

ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's members comprise the world's leading innovation companies, with headquarters worldwide. Cybersecurity is rightly a priority for all governments. We share the goal with governments of improving cybersecurity and therefore our interests are fundamentally aligned. As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. Further, our members are global companies located in various countries. Most service the global market and have complex supply chains in which products are developed, made, and assembled in multiple countries across the world. As a result, we 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.

ITI commends the Department's Internet Policy Task Force (IPTF) for its attention to the nexus of cybersecurity, innovation, and the Internet economy and for requesting comment to identify substantive cybersecurity issues that affect the digital ecosystem and digital economic growth where broad consensus, coordinated action, and the development of best practices could substantially improve security for organizations and consumers.

ITI's comments are below, both in general and in response to specific issues raised in the RFC.

General Comments

The U.S. government has a strong responsibility to make sure any cybersecurity policies we develop serve as a global model both in terms of content and process, and would be equally beneficial if deployed globally. Most of our comments and recommendations in this section will serve not only to strengthen cybersecurity and resilience in the United States, but are recommended best practices for governments globally.

ITI supports the Department of Commerce as a strong contributor to U.S. cybersecurity policies. ITI is pleased that the Department of Commerce has reinvigorated the IPTF and tasked it with working on key cybersecurity issues. Particularly given Commerce's primary role in the U.S. executive branch to promote economic growth and innovation—both of which depend on effective cybersecurity—the Department should be a key contributor to, and in many cases driver of, federal cybersecurity policies, both now and in the future.

ITI commends NTIA's open and transparent process. ITI also strongly supports the process by which NTIA is reinvigorating the IPTF. Namely, we agree with NTIA's approach to initiate an open and transparent 60-day public comment period to gather feedback from all interested stakeholders on initial ideas and proposals (as well as processes) before any work is undertaken. ITI also appreciates that all comments received will be posted in full on NTIA's website to allow for a full and inclusive discussion about next steps. This approach can help to ensure ideas are fully vetted, efforts are not duplicated, and stakeholder resources are not allocated into areas which do not warrant current action. This is a policymaking model that ITI regularly promotes when it engages foreign stakeholders.

ITI encourages NTIA to bring in global stakeholders. ITI urges NTIA, and the U.S. government generally, to conduct extensive outreach to global stakeholders, both in this public comment period and in any work processes that commence. Global outreach helps to ensure those stakeholders' views are incorporated into our work. Such an effort will likely lead to greater global consensus for cybersecurity policymaking and will help to minimize the emergence of cybersecurity policies or activities that differ radically by country. Conflicting policies would present potentially negative consequences for security, disrupt global commerce, and would ignore the borderless nature of the Internet. Transparent involvement of global stakeholders also provides a positive model to other governments that may not be as open to global input in their own policymaking.

ITI encourages NTIA to bring in stakeholders from across the United States and representing various segments of the economy. ITI urges NTIA to bring together geographically diverse stakeholders from across the United States (through geographically dispersed workshops). In addition, we encourage NTIA to bring together stakeholders representing various segments of the economy. To reach smaller companies and entrepreneurs, NTIA should leverage existing convening groups and firms (e.g., Silicon Valley-based organizations, venture capitalists, and the like).

NTIA should promote global standards and best practices. For any work related to standards (whether technology or process standards), NTIA should promote voluntary, consensus-based, industry-led, market-driven global standards. As ITI recommended when the National Institute of Standards and Technology (NIST) launched the development of the Framework for Improving Critical Infrastructure Cybersecurity (Framework), the U.S. government can set a positive example by highlighting the essential role global standards play for cybersecurity. Global standards reflect the realities of cyberspace and the ICT marketplace, facilitate global deployment of security measures, and reduce barriers to trade. Further, standardized security technologies, practices, and products deployed across the global digital infrastructure enable interoperability and assurance of security policies and controls, security innovation, efficient and effective use of private sector resources, and rapid response to cybersecurity challenges. Global standardization also restrains the emergence of multiple, conflicting security requirements in multiple jurisdictions, which could compromise cybersecurity.

NTIA should take a technology-neutral approach. As it shepherds any work processes moving forward, NTIA should not favor any particular technology or security solution. While it is understandable that the industry and market may coalesce around a particular solution, the U.S. government should follow its longstanding approach and remain neutral in these matters.

NTIA should ensure coordination with other federal efforts. NTIA should endeavor to catalog where any similar efforts are being addressed by other federal agencies (e.g. within the Department of Homeland Security (DHS), NIST, etc). If similar efforts already exist, but NTIA contributions are deemed to be useful, agencies should work together to streamline efforts to minimize redundancy.

Topics to Address

We understand that for this RFC, NTIA seeks comments on which topics to address through the process, rather than the best solution to any given question. ITI's response below highlights those topics we think deserve being addressed, along with reasoning to support each recommendation. We have copied NTIA's questions in bold italics.

NTIA proposed topic: Network and Infrastructure Security

(d) Open Source Assurance. Many organizations depend on open source projects for a wide range of purposes across the digital economy. How can stakeholders better support improving the security of open source projects, and the distribution of patches?

We recommend NTIA bring stakeholders together on this topic, although the discussion should be broadened to focus generally on best practices in software development and management, such as improving the rate of security updates across all software. Many ITI companies use both open source and proprietary software in their software development processes, and many proprietary software programs include open source components. Regardless of software type, companies employ a range of security practices throughout their software development lifecycles. A discussion among stakeholders about best practices in this space can help move the conversation beyond what type of software is "more secure" and beyond impractical proposals about the use and patching of third party and open source components in proprietary software to a discussion about how best practices in software development generally, including patching, can be shared and understood.

NTIA proposed topic: Web Security and Consumer Trust

We recommend NTIA bring stakeholders together on this general topic to discuss the state of the evolving cyber threat landscape with regard to web security and authentication. In this space, security vulnerabilities have led to identity theft, account takeovers, and cyber fraud, causing material harm for consumers in a variety of industries (for example payments, banking, retail, and tax). We believe this is an area that would benefit from a multi-stakeholder approach to assess the current landscape, with an eye toward identifying potential gaps in the public policy agenda that could be addressed via a set of voluntary consensus-based guidelines or best practices for industry. This could also be a topic where the IPTF could leverage the existing and ongoing work of others and help lead to an ultimate consensus among stakeholders.

(i) Cybersecurity and the Internet of Things. As the Internet of Things matures and more systems integrate information technologies (IT) and operational technologies (OT), cybersecurity is enmeshed in a broader risk context that includes safety, reliability, and resilience. How can we foster the emergence of voluntary policy frameworks, informed by market dynamics, that enable Internet of Things innovation while addressing the full spectrum of risks associated with cyber- physical systems?

We recommend NTIA bring stakeholders together on this topic. However, any discussions should avoid starting from the assumption that IoT somehow has different security protections/considerations from every other type of Internet Protocol (IP)-enabled device. Unfortunately, as more and more previously standalone consumer and industrial devices become networked together in the IoT, many governments are starting to consider whether IoT deserves specific policy approaches or frameworks, including in cybersecurity. We believe that in most cases, the current industry-led approaches to cybersecurity remain valid and government action to try to develop IoT-specific security policies could be harmful. Bringing together interested stakeholders to identify the applicability of ongoing cybersecurity approaches, such as existing Internet Engineering Task Force (IETF) security protocols that will naturally extend to the IoT space, identify gaps or needs related to cybersecurity in IoT, and coalesce around future action (e.g.,. research) could help advance cybersecurity in IoT.

Should NTIA decide to undertake work in this area, we have two recommendations:

- NTIA should seek to include the ICT industry as well as the various industries developing the products linked via IoT (e.g. automobiles, industrial machinery, or healthcare devices). Many IoT cybersecurity issues about which policymakers are interested—such as software development and product vulnerabilities—are not necessarily IoT-specific and there may be extensive work ongoing by the ICT industry in these areas already that can be leveraged or built upon.
- NTIA should coordinate with and leverage existing efforts on cyber-physical (IoT) systems, such as the NIST Cyber-Physical Systems Public Working Group (CPS PWG), which has been launched to bring together experts to help define and shape key aspects of CPS to accelerate its development and implementation across multiple industry sectors.[1]

(j) Privacy. As noted in the Cybersecurity Framework, privacy and civil liberties implications may arise when personal information is used, collected, processed, maintained, or disclosed in connection with an organization's cybersecurity activities. How can risks to privacy or civil liberties arising from the application of cybersecurity measures or best practices be addressed in this process (es)?

NTIA is a significant contributor to Internet policymaking both domestically and globally in connection with privacy and civil liberties. ITI sees value in NTIA continuing to utilize its role as a convener to facilitate multi-stakeholder discussions relating to the privacy and civil liberty considerations, parallel to its planned efforts on cybersecurity. We caution, however, that any such efforts should not be duplicative of other efforts currently underway within NTIA or other agencies in order to avoid redundancy and potentially contradictory outcomes.

NTIA proposed topic: Business Processes and Enabling Markets

(k) Managed Security Services: Requirements and Adoption. Managed security services (MSS) allow many firms, particularly small- and medium- sized businesses, to secure themselves without acquiring expensive in-house expertise, yet there are obstacles preventing seamless market cooperation and accountability between clients and vendors. How can a common understanding of security needs by stakeholders enable faster and more efficient adoption to improve security without sacrificing accountability?

We recommend NTIA bring stakeholders together on this topic. There are many models by which to undertake cybersecurity, including managed services and in-house security. While ITI does not advocate one method over another due to the diversity of business models practiced by our members, a discussion about the benefits of managed security services will be helpful to inform our larger efforts related to the challenges facing cross-border data flows.

As the U.S. government is aware, a growing number of governments unfortunately are proposing or enacting mandates to keep certain data within their borders under a "security" rationale (i.e., that data will be more secure if it stays within their jurisdiction). The security of data is independent of where it is stored, and in many cases, particularly for small- and medium-sized

[1] See http://www.nist.gov/cps/

business (as noted above), in-house expertise may be lacking and outsourced security, which may make sense to deliver cross-border, may be a better approach. An NTIA-led stakeholder discussion that drives greater understanding and use of managed security services could help contribute to an essential narrative to bring to the data localization debate.

NTIA might also consider facilitating a multi-stakeholder process aimed at helping SMBs to understand how to build and support more secure applications and services. Such a discussion could include application program interfaces (API), software development kits (SDK), and other secure development and programming means. In this way, the group could offer hands-on approach to SMB cybersecurity education and awareness-raising.

Should it commence work in this area, we want to voice caution about the appropriate NTIA role. NTIA should avoid activities that would seek to steer the supply side (industry's provision of solutions) or that seek to shape how industry provides and prices its managed security solutions. ITI agrees that many firms, including small- and medium-sized businesses (SMBs), might not be investing enough, or appropriately, in cybersecurity. NTIA's role should focus on helping understand the unique challenges that firms face in terms of cybersecurity solution uptake. To achieve this understanding, particularly regarding SMBs, NTIA should consult interagency among the range of peer government agencies and programs that work on a regular basis with SMBs on cybersecurity issues, including the Small Business Administration (SBA)'s Cybersecurity for Small Businesses program, NIST Manufacturing Extension Program (MEP), NIST National Cybersecurity Center of Excellence (NCCoE), and DHS's Stop.Think.Connect. Campaign.

(l) Vulnerability Disclosure. The security of the digital economy depends on a productive relationship between security vendors and researchers of all types who discover vulnerabilities in existing technology and systems, and the providers, owners, and operators of those systems. How can stakeholders build on existing work in this space to responsibly manage the vulnerability disclosure process without putting consumers at risk in the short run?

We recommend NTIA bring stakeholders together on this topic. Over recent years, policymakers in various countries have proposed requiring ICT vendors to publicize information about unpatched product vulnerabilities. Policymakers should not require, or even urge, ICT vendors to disclose product vulnerabilities before a patch to a particular vulnerability is designed and deployed. Disclosure of unpatched vulnerabilities is reckless: it puts customers at risk and reduces the effectiveness of security patches.

ITI companies take a responsible approach to disclosure of vulnerabilities to protect their customers as well as the integrity of their own systems, which include robust processes and procedures in place for timely vulnerability detection, patching, and notification as appropriate. We would be pleased to contribute our knowledge and experience to an NTIA-organized discussion with other stakeholders so that we can collectively arrive at an approach to vulnerability disclosure, supported by both vendors and consumers of ICT products. Such an approach can allow vendors or other responsible parties to manage and mitigate vulnerabilities as appropriate for the most effective cybersecurity outcomes, and allow governments and consumers to better understand the appropriate approaches to vulnerability detection, patching, and notification. Finally, NTIA should work with the State Department and other appropriate agencies to convey to global governments the risks of mandated vulnerability disclosure.

(m) Security Investment and Metrics. Market solutions for security require good information. What types of robust, practical, and actionable metrics can be used within organizations to understand security investment, and by consumers and clients to understand security practices and promote market demand for security?

The concept of metrics related to cybersecurity is complex. As ITI advised DHS in February 2014 regarding its development and implementation of a program to promote use of the NIST Framework,[2] metrics for cybersecurity must be carefully considered and approached. Cybersecurity is a process of dynamically managing risks amidst ever-evolving threats, technologies, and business models. It is important to create a "culture of security" where all stakeholders contribute to better managing their cyber risks. Attempting to quantify certain aspects of cybersecurity—such as the number of cyber incidents— may be tempting, but will not ultimately demonstrate whether stakeholders are managing cyber risks more effectively.

ITI recommended in February 2014 that any efforts to work on metrics be done in strong partnership with industry to determine the most effective ways to understand and demonstrate progress in the nearer term, and to collectively identify and evolve realistic, objective, and comparable information over the longer term.

Should NTIA decide to undertake work in this area, we have two recommendations:

- NTIA should draw from the extensive, year-long effort by the Communications Security, Reliability, and Interoperability Council (CSRIC) Working Group 4 that produced the March 2014 *Cybersecurity Risk Management and Best Practices: Final Report*.[3] CSRIC WG 4 "was given the task of developing voluntary mechanisms that give the Federal Communications Commission (FCC) and the public assurance that communications providers are taking the necessary measures to manage cybersecurity risks across the enterprise" (p. 3) and "with producing a practical, cost-effective, and segment-tailored model of risk management with **meaningful indicators to communicate assurances to internal and external stakeholders**" (p. 20, emphasis added). WG 4 concluded that "The availability of the critical infrastructure to deliver critical services is an outcome-based measure and therefore a meaningful indicator of successful cyber risk management. If issues related to availability arise as a consequence of a cyber-incident, additional examination into reliability, resiliency, and integrity of core network critical infrastructure may need to be evaluated. **Further analysis is required to determine**

[2] See "ITI recommendations to Department of Homeland Security regarding cybersecurity Voluntary Program," February 11, 2014, at http://www.itic.org/dotAsset/3ed86a62-b229-4d43-a12b-766012da4b1f.pdf
[3] https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf

whether a comprehensive and valid set of cybersecurity effectiveness metrics can be applied on a cross-sectorial basis" (p. 28, emphasis added).

- NTIA should reach out globally. A number of other governments also are grappling with the questions of cybersecurity "measurement." Including global stakeholders can help to avoid the possibility of various governments choosing different or inappropriate indicators.

Other

This list is not exhaustive. The IPTF welcomes comments on any of these topics, as well as descriptions of other topics that the IPTF and stakeholders should consider for the cybersecurity multistakeholder process. Note that comments are directly sought on which topics to address through the process, rather than the best solution to any given question.

- Global cryptographic algorithms: The global nature of technology and cyberspace underscore the essential nature of strong, robust, and globally accepted and deployed cryptographic standards to enable interoperability, trust, and security. However, an increasingly worrying trend is that of some governments mandating the use in their commercial markets of non-global cryptographic standards—China's mandate domestically of use of its SM2 standard is an example. NTIA should consider a process that engages stakeholders in a discussion of the benefits of to the digital economy, as well as security, of global cryptographic algorithms (versus national).
- Bolstering federal efforts for federal systems: There are a range of federal efforts to increase the government's own security related to the Internet. For example, the federal government currently is transitioning federal employees to computers connecting to the Internet through DNSSEC-compliant DNS servers. Although other agencies—such as DHS or the Office of Management and Budget (OMB)—are responsible for these internal efforts, NTIA could potentially play a useful role by convening a multistakeholder discussion to allow the government to learn best practices from private sector colleagues that have experienced the same transition.
- Contribute to awareness campaigns: Many federal agencies, organizations, and private-sector companies have ongoing efforts to raise awareness among all stakeholders—businesses, individual citizens, government agencies, and others--about what they can do to improve their own cybersecurity. NTIA may wish to contribute to this knowledge base by sharing appropriate outcomes from any work launched under this RFC to current campaigns. One example would be to contribute outcomes to outreach undertaken by the National Cybersecurity Alliance (NCSA), a non-profit organization focused on conducting cybersecurity education and awareness programs.

Implementing the Multistakeholder Process

In its RFC, NTIA asked for "views on how stakeholder discussions of the proposed issue(s) should be structured to ensure openness, transparency, and consensus- building." ITI provides some suggestions below.

5. How can the IPTF promote participation from a broad range of stakeholders, i.e., from industry, civil society, academia, and international partners? In particular, how can we promote engagement from small and medium-sized enterprises (SME) that play key roles in the digital ecosystem? How critical is location for meetings, and what factors should be considered in determining where to host meetings?

International partners: The IPTF should coordinate with its interagency colleagues to proactively contact Washington, DC-based foreign Embassies, leverage the officers of the Department's Foreign Commercial Service located in our Embassies and Consulates abroad who work regularly with local communities, and use multiplier groups such as associations with global memberships to try to bring these stakeholders into the discussion.

SMEs: NTIA should leverage the range of existing federal agencies and programs that work with SMEs to help them manage their cyber risks. These agencies/programs include, but certainly are not limited to, SBA's Cybersecurity for Small Businesses program, NIST MEP, NIST NCCoE, and DHS's Stop.Think.Connect. Campaign. The federal colleagues involved in those programs likely have excellent relationships with many SMEs and also an understanding of how to bring SMEs into policy discussions.

Other stakeholders - reaching out to technical experts:

- IETF engineers. Among the many engineers that we hope participate are those involved in the Internet Engineering Task Force (IETF), a large, open, international community of network designers, operators, vendors, and researchers involved in the evolution of the Internet's architecture and operation. NTIA should consider developing and using an IETF "non-working group" mailing list—these lists are very familiar platforms for engineers and allow for public discussions of various issues. This could help to include a "non-DC," more technical group of stakeholders in any work.
- Standards development organizations (SDOs). Similarly, many engineers and technical experts populate myriad SDOs working on market-driven ICT standards related to cybersecurity. NTIA should endeavor to reach out to relevant SDOs.

Location of meetings: NTIA should endeavor to hold meetings outside of the Washington, DC area. NIST's approach when developing the Cybersecurity Framework—which involved workshops around the country—helped to promote an inclusive experience and also likely enabled a larger diversity of participants than a strictly DC-based effort. Factors to consider in determining meeting locations will likely arise on a subject-by-subject or case-by-case basis, and NTIA should consult with interested stakeholders at the initial phase of launching work on any of the subjects identified in this RFC.

6. What procedures and technologies can promote transparency of process, including promoting discussion between stakeholders and ensuring those outside the process can understand the decisions made?

NTIA should follow the examples used by NIST when it led the development of the Cybersecurity Framework. In that case, NIST posted successive drafts of the Framework on its website, as well as all comments received.

CONCLUSION

ITI would like to again thank NTIA for its commitment to partnering with the private sector to improve cybersecurity. ITI also would like to commend the Administration for having integrated so much of the input it has received from industry over the past few years on this topic, and for its willingness and eagerness to consistently engage with our companies and the ICT industry generally on how government and industry can work together to improve cybersecurity. The commitment to industry outreach in this regard is an excellent example of the effective public-private partnerships that are essential to improving cybersecurity.

We hope that our comments will receive due consideration. We are available at any time to elaborate on our comments and our suggestions. ITI and its members look forward to continuing to work with NTIA and the Administration generally to improve America's cybersecurity posture. Please continue to consider ITI a resource on cybersecurity issues moving forward.

Thank you very much for your consideration.

Danielle Kriz
Director, Global Cybersecurity Policy