Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Washington, DC 20230

In the Matter of	)	
	)	
Stakeholder Engagement on Cybersecurity	)	Docket No. 150312253-5253-01
in the Digital Ecosystem	)	
	)	

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Brian Scarpelli
Director, Government Affairs

Avonne Bell
Sr. Manager, Government Affairs

David Gray
Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 North Courthouse Rd.
Suite 200
Arlington, VA 22201
(703) 907-7714

Its Attorneys

May 27, 2015

Table of Contents

I. INTRODUCTION AND SUMMARY 1

II. TIA SUPPORTS THE IPTF GOAL OF FACILITATING A SERIES OF DISCUSSIONS TO ADDRESS KEY CYBERSECURITY CHALLENGES 4

III. TIA INPUT ON MULTISTAKEHOLDER DISCUSSION STRUCTURE AND PROCESS ISSUES 8

IV. TIA INPUT ON SUBJECT AREAS OF FOCUS FOR THE IPTF MULTISTAKEHOLDER PROCESS 9

A. CYBERSECURITY AND THE INTERNET OF THINGS 9

B. MANAGED SECURITY SERVICES 12

V. CONCLUSION 13

Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Washington, DC 20230

In the Matter of	)	
	)	
Stakeholder Engagement on Cybersecurity in the Digital Ecosystem	)	Docket No. 150312253-5253-01
	)	
	)	

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

I. INTRODUCTION AND SUMMARY

The Telecommunications Industry Association ("TIA") hereby submits comments in response to the Department of Commerce Internet Policy Task Force's ("IPTF") request for 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.[1] TIA appreciates the opportunity to provide input on how the IPTF can facilitate further collaborative cybersecurity work to foster innovation and to better secure the ecosystem to ensure that businesses, organizations and individuals can expand their trust, investment and engagement in

[1] National Telecommunications and Information Administration, *Stakeholder Engagement on Cybersecurity in the Digital Ecosystem*, Request for Public Comment, 80 Fed. Reg. 14360 (Mar. 19, 2015) ("RPC")

the digital economy, while also reinforcing the voluntary, multistakeholder approach to Internet policymaking initially discussed in the Green Paper.

TIA represents hundreds of information and communications technology ("ICT") manufacturer, vendor, and supplier companies in government affairs and standards development. Numerous TIA members are companies producing ICT products and systems, creating information security-related technologies, and providing ICT services information systems, or components of information systems. These products and services innovatively serve many of the critical infrastructure sectors directly impacted by President's Executive Order[2] that created the *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* on which the Communications Security, Reliability, and Interoperability Council's ("CSRIC") Working Group 4 ("WG 4") best practices and recommendations are based.[3] To best represent the commitments of our membership in this area, TIA is an actively engaged member involved in key public-private efforts that contribute to secure information systems, including the CSRIC; the Communications Sector[4] and Information Technology Sector[5] Coordinating Councils; and the National Coordinating Center for Communications ("NCC"), the Information Sharing and Analysis Center ("ISAC") for telecommunications, part of the Department of Homeland Security's ("DHS") National Cybersecurity and Communications

---

2 *See* Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, rel. Feb. 12, 2013 ("EO 13636").

3 The National Institute of Technology and Standards (NIST), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf ("NIST Cybersecurity Framework").

4 http://www.commscc.org/

5 http://www.it-scc.org/

Integration Center;[6] among other successful public-private partnerships that the CSRIC WG 4 Report builds upon.

Through its Cybersecurity Working Group, TIA members engage in policy advocacy consistent with the following principles:

- Public-private partnerships should be utilized as effective vehicles for collaborating on current and emerging threats.
- Industry-driven best practices and global standards should be relied upon for the security of critical infrastructure.
- Voluntary private sector security standards should be used as non-mandated means to secure the ICT supply chain.
- Governments should provide more timely and detailed cyber intelligence to industry to help identify threats to protect private networks.
- Cybersecurity funding for federal research efforts should be prioritized.

TIA appreciates the National Telecommunications and Information Administration's ("NTIA") efforts to create a transparent and inclusive multistakeholder process to address key cybersecurity challenges, and looks forward to working with the IPTF and other governmental stakeholders both directly and through the envisioned multistakeholder process moving forward. In our comments below, TIA offers the following input based on the consensus views of its members:

[6] http://www.dhs.gov/national-coordinating-center-communications

- TIA supports the IPTF goal of facilitating a series of discussions to address key cybersecurity challenges;
- TIA provides input on the proposed multistakeholder discussion structure and process; and
- TIA provides support for the multistakeholder process initially addressing the topics of 'Cybersecurity and the Internet of Things' and 'Managed Security Services'

II. TIA SUPPORTS THE IPTF GOAL OF FACILITATING A SERIES OF DISCUSSIONS TO ADDRESS KEY CYBERSECURITY CHALLENGES

In the RPC, NTIA notes that the IPTF plans to facilitate a series of discussions around key cybersecurity challenges which may involve "combinations of principles, practices, and the voluntary application of policies and existing standards" while avoiding the duplication of any existing work.[7] NTIA explains that such an approach will be focused on areas where stakeholders have identified a problem or begun to seek consensus around specific practices.[8]

TIA supports such a facilitator role for the IPTF, and the proposed dialogue. Holding the experiences gained from previous and existing efforts as the development of the NIST Cybersecurity Framework (as well as the National Cybersecurity Center of Excellence ["NCCoE"] and the National Strategy for Trusted Identities in Cyberspace ["NSTIC"]), the IPTF is positioned

[7] *See* RPC at 14361.

[8] *See Id*.

in the Department of Commerce to enhance EO 13636[9] and the voluntary multistakeholder approach to cybersecurity policymaking.

TIA believes that the sole focus of IPTF-facilitated multistakeholder conversations should focus on flexible, scalable, and voluntary ways to improve cybersecurity in the digital ecosystem, and TIA opposes the multistakeholder process recommending or contemplating mandates or requirements on stakeholders. We urge the IPTF to build on EO 13636's voluntary nature, as NIST did in the development of the NIST Cybersecurity Framework. Based on the ICT manufacturer community's experience, the most effective solution to ensuring innovation in cybersecurity solutions is to rely on voluntary use of internationally-accepted standards and best practices. No part of the contemplated IPTF-facilitated multistakeholder conversations should be used to recommend or contemplate cybersecurity policies that would restrict trade in ICT equipment imported to, or exported from, other countries that are part of the global trading system.

TIA believes that any output from these multistakeholder discussions should reflect the need for cybersecurity risk management approaches in existence and under development (such as the FCC CSRIC Cybersecurity Risk Management Best Practices Report[10]) which may be tailored by individual companies to suit their unique needs, characteristics, and risks (i.e., not one-size-fits-all); are based on meaningful indicators of successful (and unsuccessful) cyber risk

---

[9] Exec. Order No. 14636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11739 (February 12, 2013), *available at* https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

[10] *See* http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf ("FCC CSRIC Cybersecurity Risk Management Best Practices Report").

management (i.e., outcome-based indicators as opposed to process metrics); and allow for meaningful assessments both internally (e.g., CSO and senior corporate management) and externally (e.g., business partners).[11] TIA fully supports the recommendations in this CSRIC-approved and FCC-endorsed report, which lays out voluntary mechanisms to provide macro-level assurance to the FCC and the public that communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks across the enterprise through the application of the NIST Cybersecurity Framework (or an equivalent construct).TIA notes that the FCC CSRIC's cybersecurity recommendations contain guidance on the cybersecurity risk management metrics[12] to which this multistakeholder discussion should defer, and upon which it should build, and which were constructed in a consensus-driven Federal advisory committee setting. While the CSRIC's recommendations apply to the communications critical infrastructure sector, they may easily serve as a model for metric discussions in other contexts.

Building on the approach of EO 13636, the Cybersecurity Framework, and the CSRIC cybersecurity risk management report, the IPTF has the opportunity to serve as a model for industry members and policymakers globally, reinforcing the success of the voluntary public-private partnership model which TIA and many others advocate as the most effective means of improving cybersecurity. In an increasing number of jurisdictions, where alternative mandate-based approaches are sometimes proposed, TIA continues to emphasize to these governments

---

[11] TIA notes that these themes guided the successful FCC CSRIC Working Group 4 report on cybersecurity risk management best practices. *See* CSRIC IV Working Group descriptions, *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_IV_Working_Group_Descriptions_9_2_14.pdf.

[12] *See* FCC CSRIC Cybersecurity Risk Management Best Practices Report at 355-367.

that the most effective solutions ensure innovation by relying on voluntary use of internationally-accepted standards and best practices, and that governments should avoid implementing cybersecurity policies that would restrict (1) trade in ICT equipment imported to, or exported from, other countries that are part of the global trading system or (2) cross-border data flows. We support the Department of Commerce's role in increasing awareness of voluntary and consensus-driven approaches to cybersecurity risk management both within the United States government as well as through government-to-government discussions and other international fora.

Finally, in undertaking these efforts, it is important that the IPTF is fully informed about and builds on existing policy and technical standardization efforts, and TIA appreciates this being underscored as a priority in the RPC. Existing efforts that will have transferability to improving cybersecurity in the digital ecosystem include the Federal Communications Commission's CSRIC WG 4 report on cybersecurity risk management, as well as numerous IoT-themed standards bodies and consortia including TIA's TR-50 (Smart Device Communications);[13] oneM2M;[14] the Internet Engineering Task Force, (IETF);[15] and the Institute of Electrical and Electronics Engineers (IEEE) Standards Association;[16] among others.

---

13 *See* http://www.tiaonline.org/all-standards/committees/tr-50.

14 *See* http://onem2m.org/.

15 *See* http://www.ietf.org/.

16 *See* http://standards.ieee.org/innovate/iot/.

III. TIA INPUT ON MULTISTAKEHOLDER DISCUSSION STRUCTURE AND PROCESS ISSUES

TIA appreciates NTIA's seeking input on how to best ensure openness, transparency, and consensus-building in the IPTF's multistakeholder process. TIA believes that it is crucial for any IPTF process building on the discussion in the RPC and public input submitted to NTIA that these characteristics be reflected. TIA provides the following views on the structure and process of the planned multistakeholder discussions:

- IPTF multistakeholder discussions should be as open and transparent as possible, allowing any impacted stakeholder to participate, whether in-person or remotely.

- IPTF should use all opportunities available to coordinate and partner within and outside of the United States government to increase awareness of its efforts. In particular, the IPTF work to ensure that international partners, both public and private, be able to participate in the discussions. TIA appreciates the coordinated roles of the IPTF and NIST (and other government stakeholders) in addressing policy and technical/standardization efforts in the cybersecurity space.

- TIA, with a membership comprised of ICT businesses of all sizes, understands and appreciates that small businesses, while a crucial driver of the American economy, may not have broad awareness of the Framework, nor have the resources to invest in the prevention of cyber attacks to the degree that larger organizations do. For small businesses, the importance of education and public awareness in efforts to improve resiliency to cyber-based attacks is especially crucial. These educational efforts, ideally coordinated across the government, will aid small businesses in understanding cybersecurity threats, increase awareness of existing helpful resources available from the government, and help explain how these resources can be best utilized (*e.g.*, how to use the NIST Framework). Holding a series of workshops in different regions of the United States, as proposed in the RPC, will likely encourage increased in-person participation from small- and medium-sized entities ("SMEs"). When selecting physical locations for meetings, TIA suggests considering those locations with lower costs and greater accessibility for SMEs.

IV. TIA INPUT ON SUBJECT AREAS OF FOCUS FOR THE IPTF MULTISTAKEHOLDER PROCESS

TIA appreciates the Administration's efforts to enhance voluntary participation in enhanced cybersecurity practices, and understands that, initially, NTIA seeks to determine two to three subject areas for initial focus. Towards identifying these subject areas of highest stakeholder interest of those put forward in the RPC which would benefit from a multistakeholder process, TIA elaborates below on how the multistakeholder process would particularly benefit the topics of (1) 'Cybersecurity and the Internet of Things'; and (2) 'Managed Security Services'.

A. Cybersecurity and the Internet of Things

In TIA's view, the future for telecommunications and the world economy lies with the Internet of Things ("IoT"). At its most basic, the "Internet of Things" is a label for an increasingly connected future in which regular, everyday items – from household appliances to cars to medical devices – are outfitted with sensors and connected to the Internet to share their data. Viewed more broadly, the Internet of Things will give rise to an entire ecosystem for interconnected devices, objects, systems, and data all working together. In this new world, most communications will be machine-to-machine (M2M), and there will be a continuous exchange of information between devices, sensors, computers, and networks.

Aside from driving transformative societal effects, the economic potential of the IoT is enormous. In 2012, an estimated 8.7 billion "things" were connected worldwide, and projections show that this could grow to 50 billion by the year 2020[17] – generating global

[17] http://share.cisco.com/internet-of-things2.html

revenues of $8.9 trillion in the process.[18] In direct terms, this represents an enormous market for ICT manufacturers, vendors, and suppliers. Ultimately, however, there will be enormous secondary economic effects as the Internet of Things emerges and gradually transforms daily life worldwide.

Recognizing that policymakers are taking a much greater interest in the IoT and are attempting to craft forward-looking laws and regulations that keep pace with innovation (or at least do not hinder it), TIA has developed *Realizing the Potential of the Internet of Things: Recommendations to Policy Makers*,[19] a white paper offering a general framework for these IoT policy discussions, which we released during a March 26 roundtable event.[20] In this white paper, TIA recommends that when addressing data security and resilience, policymakers should ensure respect for competitive differentiation as a primary driver of enhanced security solutions, rely on international standards and best practices, fully leverage the public-private partnership model, and to prioritize end-user awareness and education.[21]

In its white paper, TIA also underscores how, with numerous areas of priority running across IoT applications and use cases (ranging from interoperability to privacy to data security), a significant danger exists that vertical approaches imposed in one market will be inappropriate for another. This could lead to a balkanized regulatory approach that stifles innovation and delays or degrades the economic and social potential of the IoT. It is crucial for the United

---

18 http://www.idc.com/getdoc.jsp?containerId=prUS24366813

19 http://www.tiaonline.org/sites/default/files/pages/TIA-White-Paper-Realizing_the_Potential_of_the_Internet_of_Things.pdf

20 http://www.tianow.org/videos/internet-of-things-roundtable-with-industry-leaders/14100

21 *See* TIA IoT White Paper at 8-11.

States government to develop an IoT strategy to prevent this balkanization, and this need could be addressed (from the cybersecurity perspective) through the multistakeholder process.

Based on the above, TIA agrees that enhancing cybersecurity in the IoT, particularly as more systems integrate information technologies (IT) and operational technologies (OT), could benefit from the multistakeholder discussion as envisioned by NTIA in the RPC. This activity would also be supported in the President's National Security Telecommunications Advisory Committee (NSTAC) report on the IoT and its impact to national security and emergency preparedness, which recommends the close collaboration of government and industry to "coordinate, collaborate and leverage the various industry IoT consortia to develop, update, and maintain IoT deployment guidelines to manage cybersecurity implications and risks."[22]

Given the potential of the IoT, TIA believes that addressing this topic in a multistakeholder discussion would benefit the digital ecosystem as a whole. As noted above (and by NTIA in the RPC), the outcome of such a discussion and any outcome will be dependent on the issues discussed within the process. However, TIA believes that such discussions will be additive to common priority of increasing cybersecurity in the IoT as long as the goals of the effort remain focused on the emergence of voluntary policy frameworks.

Importantly, the multistakeholder discussion should serve an important role in ensuring IoT data privacy through public awareness efforts. Through "cyber hygiene" education efforts, many breaches that would result in a loss of data privacy can be avoided, and a more informed

[22] *See* NSTAC, NSTAC Report to the President on the Internet of Things (Feb. 19, 2014), *available at* http://www.dhs.gov/sites/default/files/publications/Final%20NSTAC%20Industrial%20Internet%20Scoping%20Report_0.pdf.

end-user is less likely to make voluntary decisions with IoT devices and services that allow data usage beyond their individual comfort.

B. Managed Security Services

Increasingly, businesses across multiple sectors of the economy have begun to rely on outsourced managed security services ("MSS") to ensure business continuity. These services typically include continuous network monitoring, administration of attack recognition tools, patching of systems, security evaluations audits, and attack response/mitigation. TIA agrees that MSS may be of particular benefit to small- and medium-sized businesses by letting these organizations avoid having to acquire in-house staff, but also are increasingly used (either in part or completely) by large organizations as well. An increasing number of TIA's members have begun to offer these services, and TIA believes that the growth of the MSS market will further increased resilience to cyber-based attacks by providing scalable options in the marketplace. Based on the above, TIA supports the proposal to initiate, and would be interested in contributing our views and experiences on, open multistakeholder dialogue on MSS best practices, towards enabling increased adoption of improved security for organizations of all sizes, while also improving accountability.

V. CONCLUSION

TIA appreciates the Commission's consultation regarding these possible rule revisions, and urges consideration of the recommendations above. We stand ready to work with the IPTF in its work on cybersecurity issues that affect the digital ecosystem and digital economic growth.

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Brian Scarpelli
Director, Government Affairs

Avonne Bell
Sr. Manager, Government Affairs

David Gray
Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 North Courthouse Rd.
Suite 200
Arlington, VA 22201
(703) 907-7700

Its Attorneys

May 27, 2015