

In the Matter of

)

**Stakeholder Engagement on Cybersecurity
in the Digital Ecosystem**

)

Docket No. 150312253-5253-01

)

)

**COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION**

Robert Mayer
Kevin G. Rupy
United States Telecom Association
607 14th Street, N.W.
Suite 400
Washington, D.C. 20005
(202) 326-7200

May 27, 2015

TABLE OF CONTENTS

I. Introduction	1
II. Broad Participation from Stakeholders in the Digital Ecosystem is Essential to Effectively Address Specific Cybersecurity Challenges.....	4
III. The NIST Framework Serves as an Exemplary Model for the Open, Voluntary and Stakeholder-Driven Process that NTIA Seeks to Implement	5
IV. NTIA Projects Should Complement or Replace Efforts in Other Venues to Ensure that Critical Resources are Not Squandered	6
V. NTIA Can Achieve the Greatest Impact by Focusing on Narrowly-Defined Threats Within Discrete Cybersecurity Areas	7
VI. Remarks on Specific Topics.....	8
A. Botnet and Malware Mitigation (combined)	9
B. Trust and Security in Core Internet Infrastructure/Domain Name Server (DNS), Border Gateway Protocol, and Transport Layer Security Certificates (combined)	11
C. Cybersecurity and the Internet of Things (IoT).....	13
VII. Conclusion	16

* * *

Summary

USTelecom appreciates the Department of Commerce's continuing interest in protecting our nations' vital economic security and reaffirming its earlier finding that evolving cybersecurity threats pose significant societal risk and that "the pace of innovation in the highly digital ecosystem makes traditional regulation and compliance difficult and inefficient." The current Request takes note of several key developments that have occurred since the release of the Department's 2011 Green Paper, all of which have important bearing on the issues raised in this inquiry.

For example, in September 2011, the Department and the Department of Homeland Security issued a Notice of Inquiry regarding existing efforts and new areas to explore in combating botnets and related malware. Largely as a consequence of that inquiry, the private sector formed the Industry Botnet Group (IBG) which operated as a voluntary public-private partnership comprised of nine trade associations and nonprofit organizations representing thousands of companies across information, communications, and financial services industries. This effort produced findings and recommendations that can be leveraged as part of any further effort facilitated by the National Telecommunications and Information Administration (NTIA).

In addition, in February 2013, the White House released Executive Order 13636 which had a profound impact on shaping and advancing the relationship between government and industry in the cybersecurity arena. The Executive Order set in motion a year-long National Institute of Standards and Technology (NIST) led engagement to develop a cybersecurity framework (CSF) that was well-organized, managed, and facilitated. The NIST effort led to the production of a landmark business-driven cyber risk management tool that is reverberating through multiple industry and government venues.

The CSF served as the foundational cornerstone for a subsequent groundbreaking initiative by the communications sector with the release of the Communications Security, Reliability and Interoperability Council (CSRIC) Working Group 4 (WG 4) report in March 2015. Both the NIST Framework and the CSRIC WG4 initiatives have served to significantly enhance the cybersecurity landscape by promoting voluntary, multi-stakeholder collaborative mechanisms and approaches that address one of the most urgent challenges we face as a nation. Furthermore, they can serve as a useful model for much of what the National Telecommunications and Information Administration (NTIA) hopes to accomplish in its important upcoming work.

USTelecom maintains that broad participation from stakeholders in the digital ecosystem is essential to effectively addressing specific cybersecurity challenges. The Internet ecosystem was a major focus area in a recent CSRIC WG4 effort to adapt the NIST Cybersecurity Framework to various communication segments, and a sub-group leading this effort identified 27 unique ecosystem categories (*e.g.*, hardware vendors, operating-system vendors, backbone network operators) that together form a complex system of cybersecurity interdependencies. A clear take-away from this effort was that effective management of cybersecurity risk requires significant participation from multiple stakeholders from the enterprise level up through the broader sector level. NTIA is in a unique position to convene and facilitate this type of

engagement on a number of timely and critical issues affecting Internet security.

USTelecom applauds the NTIA Internet Policy Task Force (IPTF) in its efforts to facilitate one or more multi-stakeholder processes based on “openness, transparency, and consensus” which were the hallmarks of the NIST CSF development process. Most importantly, the NIST team paced the effort to allow sufficient time for stakeholders to review progress and provide substantive public input at regular intervals, while still managing a complex effort to an aggressive timeline. By incorporating lessons learned from the NIST engagement, the IPTF will increase the likelihood of successful engagements.

NTIA should consider its appropriate role in the broader coordination context of cybersecurity efforts. As NTIA acknowledges in its Request, it seeks to “avoid duplicating existing work,” and focus instead on designing processes that “complement, rather than duplicate existing initiatives, both inside and outside the government.” NTIA should therefore consider greater collaboration with existing government cybersecurity related entities, including the National Science Foundation and NIST, as well as DHS. In particular, DHS is the lead agency for the Critical Infrastructure Partnership Advisory Council (CIPAC) which facilitates interaction between governmental entities and representatives from the community of critical infrastructure owners and operators. The value of these organizations and efforts will be significantly enhanced by NTIA’s leadership and expertise in the communications arena.

There is broad agreement among all stakeholders – including NTIA – that the cybersecurity landscape is a multi-faceted environment with numerous threat vectors, vulnerabilities and response mechanisms. Given the inherent complexities within this environment, NTIA should carefully scope its efforts by focusing on narrowly defined threats within discrete cybersecurity areas.

Botnet and Malware Mitigation

There is no dispute that one of those most persistent threats to the global digital economy comes from the proliferation of destructive botnets and malicious software (malware) that, among other things, enables a single entity to control large networks of infected computers. Though most commonly associated with criminal enterprise and financial theft in particular, botnets can also be used for cyber espionage and potential attacks by terrorist or nation states to disrupt major economic activity or to attack vital critical infrastructure. USTelecom members and other sector participants have been major contributors in foundational efforts that brought key stakeholders together to address important issues and responsibilities.

These efforts include the voluntary U.S. Anti-Bot Code of Conduct (“Code of Conduct”) for Internet Service Providers (ISPs) to address threats posed to residential broadband networks, as well as efforts of the IBG, which developed principles to guide voluntary anti-botnet efforts throughout the ecosystem. USTelecom asserts that a starting point for further progress in this area could entail further expansion of a set of voluntary practices that can be developed and applied to the broad set of ecosystem stakeholders identified in the IBG. Building upon the principles identified in the IBG, NTIA could function as an effective facilitator to orchestrate the high-level of ecosystem engagement that will increase the likelihood of achieving further progress in the areas of botnet and malware mitigation.

Trust and Security in Core Internet Infrastructure/Domain Name Server (DNS), Border Gateway Protocol, and Transport Layer Security Certificates

The Request captures a number of potential areas where collective action to advance Internet security is both necessary and possible. While USTelecom does not propose recommendations for specific technical engagements in these areas at this time, there are foundational activities that can be undertaken to advance NTIA's stated objectives. There are many other prominent venues where standards and guidelines have been developed or are currently under development. Many of these organizations are identified in a Government Accountability Office (GAO) report "Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use." NTIA could take a significant step towards understanding the factors that have influenced adoption and diffusion to date by designing a well-structured, multi-stakeholder engagement to clarify what actions have been taken, where those actions have been taken, the conclusions that have been reached, and the lessons learned from their implementation across multiple sectors. More importantly, such an inquiry could have the added benefit of providing further insight into potential synergies that result from collective action in engagement in these areas.

Cybersecurity and the Internet of Things (IoT)

The IoT presents society with an unparalleled level of cybersecurity issues, given its sustained exponential growth, and the diversity of stakeholders who will develop, market and use IoT-enabled devices and applications. What makes IoT particularly challenging from a cybersecurity perspective is that all of the factors that contribute to current vulnerabilities and concerns (e.g., accelerated market entry, cost reduction, insufficient security-by-design, and privacy) are increased by orders of magnitude.

One of the primary goals of a policy framework for IoT should be to ensure that, while innovation remains unimpeded, security considerations and voluntary practices are incorporated into multiple dimensions of the risk landscape. This is especially the case given what is currently known about the IoT environment. Given the security implications, USTelecom members understand that security is essential for the growth of business and commerce in the IoT space. For this reason, they are working on crucial security standards in a variety of venues to ensure such measures are resident in any future IoT offerings.

NTIA can play a crucial role in this area by promoting the use of the various solutions developed through organizations such as the ATIS and the GSMA throughout broader industry segments. For example, NTIA could promote use of such solutions by highlighting some specific use cases around various IoT industries such as automotive, healthcare information technology, utilities and others. NTIA must also ensure that any policy framework it implements is sufficiently flexible to accommodate new information related to evolving market dynamics, stakeholder resource concerns and business models, infrastructure and operating environments, end-user expectations and awareness, and laws and regulations. NTIA should begin the development of its policy framework with a set of consensus-based principles that could help guide the identification and formulation of appropriate policy considerations.

In the Matter of)
Cybersecurity, Innovation and the) Docket No.: 110527305–1303–02
Internet Economy)

**COMMENTS OF
THE UNITED STATES TELECOM
ASSOCIATION**

The United States Telecom Association (USTelecom)¹ is pleased to comment on the Request for Public Comments (*Request*) issued by the Department of Commerce (Department) regarding its inquiry “to identify substantive cybersecurity issues that affect the digital ecosystem.”² USTelecom agrees with the Department’s assessment that “broad consensus, coordinated action, and the development of practices could substantially improve security for organizations and consumers.”³

I. Introduction

USTelecom appreciates the Department’s continuing interest in protecting our nations’ vital economic security and reaffirming its earlier finding that evolving cybersecurity threats pose significant societal risk and that “the pace of innovation in the highly digital ecosystem makes traditional regulation and compliance difficult and inefficient.”⁴ The current Request

¹ USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks.

² See, Request for Public Comment, *Stakeholder Engagement on Cybersecurity in the Digital Ecosystem*, FR / Vol. 80, No. 53 / Thursday, March 19, 2015) (available at: http://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03192015.pdf (visited May 10, 2015) (*Request*).

³ *Request*, p. 14360.

⁴ See, The Department of Commerce Internet Policy Task Force, *Cybersecurity, Innovation and the Internet Economy*, June, 2011 (available at:

takes note of several key developments that have occurred since the release of the Department's 2011 Green Paper,⁵ and we believe these activities have important bearing on the issues raised in this inquiry.

The Request notes that in September 2011, a Notice of Inquiry was issued from the Department and the Department of Homeland Security (DHS) to learn more about existing efforts and new areas to explore in combating botnets and related malware.⁶ Largely as a consequence of that inquiry, the private sector formed the Industry Botnet Group (IBG) which operated as a voluntary public-private partnership comprised of nine trade associations and nonprofit organizations representing thousands of companies across information, communications, and financial services industries.⁷ This effort, which was formed in close coordination among the White House Cybersecurity Office, the Department, DHS and private industry, produced findings and recommendations that are discussed in these comments and can be leveraged as part of any further effort facilitated by the National Telecommunications and Information Administration (NTIA).

In February 2013, the White House released Executive Order 13636 ("the Executive Order"), which had a profound impact on shaping and advancing the relationship between

http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf (*Green Paper*) (visited May 19, 2015).

⁵ Department Of Commerce, Internet Policy Task Force, *Cybersecurity, Innovation and The Internet Economy*, June 2011 (available at: http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf) (visited May 21, 2015).

⁶ Notice of Inquiry, U.S. Department of Commerce and U.S. Department of Homeland Security, *Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware*, 76 FR 58466 (September 21, 2011) (available at: http://www.ntia.doc.gov/files/ntia/publications/botnet_rfi.pdf) (visited May 19, 2015).

⁷ See, Department of Commerce Press Release, *White House Announces Public-Private Partnership Initiatives to Combat Botnets*, May 30, 2012 (available at: <http://2010-2014.commerce.gov/news/press-releases/2012/05/30/white-house-announces-public-private-partnership-initiatives-combat-b>) (visited May 19, 2015).

government and industry in the cybersecurity arena.⁸ The Executive Order cemented the critical role of the public-private partnership model stating that “it is the policy of the United States to enhance the security and resilience of the nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. *We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.*”⁹

Most significantly, the Executive Order set in motion a year-long National Institute of Standards and Technology (NIST) led engagement to develop a cybersecurity framework (CSF) that was well-organized, managed, and facilitated. The NIST effort led to the production of a landmark business-driven cyber risk management tool that is reverberating through multiple industry and government venues.¹⁰ As recently reported in a National Law Review article, “without question, the Framework has sparked a national conversation about cybersecurity and the controls necessary to improve it.”¹¹

The CSF served as the foundational cornerstone for a subsequent groundbreaking initiative by the communications sector with the release of the Communications Security,

⁸ Exec. Order No. 13636, *Improving Critical Infrastructure Cybersecurity*, 78 FR 11739 (February 12, 2013) (available at: <https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructurecybersecurity>) (*Executive Order*) (visited May 19, 2015).

⁹ *Executive Order*, Section 1, Policy (emphasis added).

¹⁰ See, National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*, (February 12, 2014) (available at: <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>) (visited May 21, 2015).

¹¹ See, Ann Killilea, Amy C.Pimentel, The National Law Review, *Where Are We Now? The NIST Cybersecurity Framework One Year Later*, 2015 (available at: <http://www.natlawreview.com/print/article/where-are-we-now-nist-cybersecurity-framework-one-year-later>) (visited May 21, 2015).

Reliability and Interoperability Council (CSRIC) Working Group 4 (WG 4) report in March 2015.¹² This effort involved over 100 cybersecurity professionals who worked for over a year to produce recommendations, guidance and analyses that have been widely recognized as a significant contribution to advance cybersecurity risk management capabilities across the entire communications sector.¹³ Some of the key lessons-learned and findings contained in the WG-4 report serve as an input into our remarks below on specific topics. Both the NIST Framework and the CSRIC WG4 initiatives have served to significantly enhance the cybersecurity landscape by promoting voluntary, multi-stakeholder collaborative mechanisms and approaches that address one of the most urgent challenges we face as a nation. Furthermore, they can serve as a useful model for much of what NTIA hopes to accomplish in its important upcoming work.

II. Broad Participation from Stakeholders in the Digital Ecosystem is Essential to Effectively Address Specific Cybersecurity Challenges

The Internet ecosystem was a major focus area in a recent CSRIC WG4 effort to adapt the NIST Cybersecurity Framework to the broadcast, cable, satellite, wireless and wireline segments.¹⁴ The analysis was used as a basis for understanding ecosystem dependencies as they impacted cybersecurity risk management considerations for the sector. The WG4 sub-group that led this effort identified 27 unique ecosystem categories (*e.g.*, hardware vendors, operating-system vendors, backbone network operators) that together form a complex system of cybersecurity interdependencies. The sub-group members also noted that cyber-attacks had been

¹² See, The Communications Security, Reliability and Interoperability Council (CSRIC) IV, Working Group 4: Final Report, *Cybersecurity Risk Management and Best Practices*, March 2015 (available at: <http://www.natlawreview.com/print/article/where-are-we-now-nist-cybersecurity-framework-one-year-later>) (*CSRIC IV Report*) (available at: https://transition.fcc.gov/pshs/advisory/csrc4/CSRIC_IV_WG4_Final_Report_031815.pdf) (visited May 21, 2015).

¹³ See, Remarks by FCC Chairman Thomas Wheeler, RSA Conference, April 21, 2015 (available at: http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0421/DOC-333127A1.pdf) (visited May 21, 2015).

¹⁴ See *e.g.*, *CSRIC IV Report*, pp. 321 - 355.

observed and mapped to every layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) communications model and against every identified category of the ecosystem. A clear take-away from the findings was that effective management of cybersecurity risk requires significant participation from multiple stakeholders from the enterprise level up through the broader sector level.

NTIA is in a unique position to convene and facilitate this type of engagement on a number of timely and critical issues affecting Internet security. A key component of the agency's mission statement is "ensuring that the Internet remains an engine for continued innovation and economic growth."¹⁵ It is vital to the success of any future engagement that project participants include representatives from the industry segments and organizations that have responsibility for managing their piece of the cybersecurity risk management puzzle. USTelecom asserts that this one factor is the sine qua non for any work to make a difference and to have a chance for tangible and actionable outcomes. NTIA may need to engage in aggressive outreach to encourage the requisite level of participation.

III. The NIST Framework Serves as an Exemplary Model for the Open, Voluntary and Stakeholder-Driven Process that NTIA Seeks to Implement

USTelecom applauds the NTIA Internet Policy Task Force (IPTF) in its efforts to facilitate one or more multi-stakeholder processes based on "openness, transparency, and consensus"¹⁶ which were the hallmarks of the NIST CSF development process. That effort was praised by a large group of diverse stakeholders for its inclusiveness and its continuous and regular engagement with industry.

Most importantly, the NIST team paced the effort to allow sufficient time for

¹⁵ See, NTIA website, *About NTIA* (available at: <http://www.ntia.doc.gov/about>) (visited May 21, 2015).

¹⁶ Request, p. 14361.

stakeholders to review progress and provide substantive public input at regular intervals, while still managing a complex effort to an aggressive timeline. Holding six multi-day workshops in various locations throughout the country ensured greater interaction and participation by subject matter experts who might otherwise not have been able to attend. By incorporating these and other lessons learned from the NIST engagement, the IPTF will increase the likelihood of successful engagements.

IV. NTIA Projects Should Complement or Replace Efforts in Other Venues to Ensure that Critical Resources are Not Squandered

There are several ways for NTIA to achieve its goal of facilitating multistakeholder discussions that will be a “catalyst for self-coordination of cybersecurity activities.”¹⁷ First, NTIA should consider its appropriate role in the broader coordination context of cybersecurity efforts. As NTIA acknowledges in its Request, it seeks to “avoid duplicating existing work,”¹⁸ and focus instead on designing processes that “complement, rather than duplicate existing initiatives, both inside and outside the government.”¹⁹

In the coordination context, the Intelligence and National Security Alliance (INSA) has noted that with respect to the global cybersecurity environment, “[l]aws, standards and technology cannot simply be levied against such an integrated system of networks. Questions over roles, responsibilities, and jurisdictional boundaries only become more prolific as we strive to clarify them.”²⁰ As a key stakeholder in the cybersecurity environment, such a role is well suited for NTIA which can complement existing coordination efforts by other critical

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Request*, p. 14361.

²⁰ Intelligence and National Security Alliance Report, *Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models*, p. 4, November, 2009 (available at: http://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx) (visited May 21, 2015).

agencies. The importance of interagency coordination has been previously identified by the White House as a key component to the nation's cybersecurity action plan.²¹

NTIA should therefore consider greater collaboration with existing government cybersecurity related entities. These entities include the National Science Foundation and NIST,²² as well as DHS which brings together various government organizations and industry partners through a variety of cybersecurity-related programs. In particular, DHS is the lead agency for the Critical Infrastructure Partnership Advisory Council (CIPAC) which facilitates interaction between governmental entities and representatives from the community of critical infrastructure owners and operators.²³ The value of these organizations and efforts will be significantly enhanced by NTIA's leadership and expertise in the communications arena.

V. NTIA Can Achieve the Greatest Impact by Focusing on Narrowly-Defined Threats Within Discrete Cybersecurity Areas

There is broad agreement among all stakeholders – including NTIA – that the cybersecurity landscape is a multi-faceted environment with numerous threat vectors,

²¹ See, White House Report, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*, p. 37, June, 2009 (identifying as a near term action plan the convening of appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulating coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government) (available at: https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf) (visited May 21, 2015).

²² NIST is engaged in various activities that are consistent with areas of expertise inherent in the Department's ongoing activities. This includes NIST's Smart Grid Interoperability Project, as well as projects relating to cybersecurity. See e.g., NIST Press Release, *Commerce Secretary Unveils Plan for Smart Grid Interoperability*, released September 24, 2009 (available at: http://www.nist.gov/public_affairs/releases/smartgrid_092409.html) (visited May 21, 2015); see also, NIST Press Release, *NIST Releases Final Version of New Cybersecurity Recommendations for Government*, released July 24, 2009 (available at: http://www.nist.gov/itl/csd/sp800-53iii_081109.cfm) (visited May 21, 2015).

²³ DHS website, *Critical Infrastructure Partnership Advisory Council* (available at: <http://www.dhs.gov/critical-infrastructure-partnership-advisory-council>) (visited May 20, 2015).

vulnerabilities and response mechanisms. Given the inherent complexities within this environment, NTIA should carefully scope its efforts by focusing on narrowly defined threats within discrete cybersecurity areas. In each of the proposed topics we discuss below, we offer some ideas as a starting point for a focused NTIA and stakeholder-framed inquiry. Such an approach will ensure that NTIA and participating stakeholders attain actionable results, while better economizing existing resources.

Given the favorable implications that adoption of narrowly tailored approaches will have for ensuring increased cybersecurity, NTIA should develop and implement such approaches in this area. Such narrowly tailored approaches will afford all stakeholders sufficient flexibility to address the unique circumstances arising in this area.

VI. Remarks on Specific Topics

The Request identifies 13 potential topic areas organized around three major groupings: 1) Network and Infrastructure Security; 2) Web Security and Consumer Trust; and 3) Business Processes and Enabling Markets. Commenters are asked to explain why, or why not, an individual topic may be a good fit for a multi-stakeholder process, why such a process would benefit the ecosystem, and what form an actionable outcome may take. They are also asked to comment on how-long a “facilitated, participant-led process” should take to come to consensus and what pre-existing work already exists on the topic.

Many, if not all, of the proposed topics have merit, but USTelecom’s comments focus on those topics that it believes are most relevant, best suited for a collaborative, multi-stakeholder process and have a relatively high probability for producing tangible and actionable outcomes. However, USTelecom avoids speculating on how long a topic area might take to achieve consensus knowing that this will be a function of multiple factors such as how each topic area problem is ultimately defined, the breadth of ecosystem participation, stakeholder consensus around desired outcomes, and effectiveness of facilitating the process. Moreover, USTelecom

believes that the projects that are selected in the first round of activities should be scoped to produce results within a relatively short period (perhaps one year) to prove the effectiveness of the venue and knowing that such a benchmark had been set with the development of the NIST Framework and the WG4 effort. The topic areas discussed below meet the criteria described above and are presented in no particular rank order.

A. Botnet and Malware Mitigation (combined)

There is no dispute that one of those most persistent threats to the global digital economy comes from the proliferation of destructive botnets and malicious software (malware) that, among other things, enables a single entity to control large networks of infected computers. Though most commonly associated with criminal enterprise and financial theft in particular, botnets can also be used for cyber espionage and potential attacks by terrorist or nation states to disrupt major economic activity or to attack vital critical infrastructure.

Testifying before Congress last year, the FBI's Assistant Director of the Cyber Division, Joseph Demarest cited estimates that botnets have caused over \$9 billion in losses to U.S. victims and over \$110 billion in global losses. He maintained that approximately 500 million computers are infected globally each year, translating into 18 victims per second.²⁴

The botnet and malware mitigation problems have spurred several major initiatives over the years to facilitate accountability and engagement. USTelecom members and other sector participants have been major contributors in foundational efforts that brought key stakeholders together to address important issues and responsibilities.

In March 2012, under the auspices of CSRIC III, an industry working group delivered the voluntary U.S. Anti-Bot Code of Conduct ("Code of Conduct") for Internet Service

²⁴ See, Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Joseph Demarest, Assistant Director, Cyber Division, Federal Bureau of Investigation, July 15, 2014 (available at: <http://www.fbi.gov/news/testimony/taking-down-botnets>) (visited May 21, 2015).

Providers (ISPs) to address threats posed to residential broadband networks.²⁵ Under the Code of Conduct, ISPs agreed to educate consumers about the botnet threat, take steps to detect botnet activity on their networks, make consumers aware of botnet infections on their computers, offer assistance to consumers whose computers are infected, and collaborate with other service providers that have also adopted the Code of Conduct. A key finding of that effort was that “constituents of the entire Internet ecosystem have important roles to play in addressing the botnet threat and that ISPs depend on support from the other parts in the ecosystem.”²⁶

The Industry Botnet Group (IBG) was an example of another major initiative where USTelecom played a contributing role in facilitating further multi-stakeholder dialogue to address the issues around botnets. The IBG brought together a larger stakeholder community with a specific set of goals that included the development of principles to guide voluntary anti-botnet efforts throughout the ecosystem.²⁷ In May 2012, the IBG presented its work at a White House event where the group presented nine principles to govern future engagement across the

²⁵ See, The CSRIC Council II, Working Group 7, Final Report, *U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)*, March 2012 (available at: <https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf>) (visited May 21, 2015), see also, The CSRIC II, Working Group 7, Final Report, *U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs), Barrier and Metric Considerations*, March 2013 (available at: https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf) (*CSRIC Metric Considerations Report*) (visited May 21, 2015).

²⁶ *CSRIC Metric Considerations Report*, p. 3.

²⁷ See, USTelecom blog, *The Industry Botnet Group Takes Multi-Party Approach to Fight Cybercrime*, May 30, 2012 (available at: <http://www.ustelecom.org/blog/industry-botnet-group-takes-multi-party-approach-fight-cybercrime>) (visited May 26, 2015).

ecosystem.²⁸ A fundamental finding of the group was that addressing botnets is a shared responsibility and that all stakeholders have a role to play.²⁹

While other venues exist where important work has been undertaken to address botnet and malware mitigation issues, there remains a need for further multi-stakeholder engagement.³⁰ USTelecom asserts that a starting point for further progress in this area could entail further expansion of a set of voluntary practices that can be developed and applied to the broad set of ecosystem stakeholders identified in the IBG. Building upon the principles identified in the IBG, NTIA could function as an effective facilitator to orchestrate the high-level of ecosystem engagement that will increase the likelihood of achieving further progress in the areas of botnet and malware mitigation.

B. Trust and Security in Core Internet Infrastructure/Domain Name Server (DNS), Border Gateway Protocol, and Transport Layer Security Certificates (combined)

The Request captures a number of potential areas where collective action to advance Internet security is both necessary and possible. While USTelecom does not propose recommendations for specific technical engagements in these areas at this time, there are foundational activities that can be undertaken to advance NTIA's stated objectives. USTelecom

²⁸ Travis Hessman, Industry Week, *Nine Principles to Boost Cybersecurity*, May 31, 2012 (available at: <http://www.industryweek.com/information-technology/nine-principles-boost-cybersecurity?page=2>) (visited May 21, 2015).

²⁹ The IBG identified the following key constituencies: Anti-virus and security vendors, application and operating system developers, device manufacturers, domain registrars and registries, end users, Internet service and cloud service providers, IT departments, public-private partnerships, search engines, website owners and others.

³⁰ See, work of Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) website, New M3AAWG Bot Metrics Report Shares Network Operators' Perspective, October 20, 2014 (available at: <https://www.m3aawg.org/dm3z/2014/10/20/new-m3aawg-bot-metrics-report-shares-network-operators%20%99-perspective>) (visited May 21, 2015); see also M³AAWG website, *MAAWG Tackles Bots with New ISP Guidelines for Restoring Infected End-Users' Machines* (available at: https://www.m3aawg.org/media_center/maawg-tackles-bots-with-new-isp-guidelines-for-restoring-infected-end-users-machines) (visited May 21, 2015).

notes that a significant amount of work has already been undertaken or is underway in many of these areas. For example, the communications sector has addressed core Internet infrastructure and security improvements and best practices in multiple CSRIC-chartered working groups over the past several years.³¹ These reports are indicative of the substantial investment of resources that the communications sector has made in investigating these issues and this is a good time to broaden the breadth of stakeholder participation.

There are many other prominent venues where standards and guidelines have been developed or are currently under development. Many of these organizations are identified in a Government Accountability Office (GAO) report “Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use.” The GAO report makes note of the fact that an abundant body of work already exists across scores of entities and that “given the plethora of guidance available, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture. Improved

³¹ See, The CSRIC III, Working Group 5, *Final Report on Measurement of DNSSEC Deployment, Version 11*, February 22, 2013 (available at: https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG5_Report_March_2020_13.pdf) (visited May 21, 2015); see also, The CSRIC III, Working Group 4, Network Security Best Practices, *Final Report – BGP Security Best Practices*, March, 2013 (available at: https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_2020_13.pdf) (visited May 21, 2015); The CSRIC III, Working Group 6, *Final Report, Secure BGP Deployment*, March, 2013 (available at: https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_2020_13.pdf) (visited May 21, 2015); see also, The CSRIC, Working Group 6, *Final Report, Long-Term Core Internet Protocol Improvements*, September, 2014 (available at: https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_2020_13.pdf) (visited May 21, 2015); see also, The CSRIC III, Working Group 4, Network Security Best Practices, *Final Report, DNS Best Practices*, September 2012 (available at: https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_9-12-12_WG4-FINAL-Report-DNS-Best-Practices.pdf) (visited May 21, 2015).

knowledge of the guidance that is available could help both federal and private sector decision makers better coordinate their efforts to protect critical cyber-reliant assets.”³²

NTIA has appropriately narrowed the focus of possible engagements in these areas by asking “what collective action can be taken to promote the voluntary adoption and diffusion of existing technical solutions to make the infrastructure more trustworthy?”³³ While there is an extensive inventory of existing technical solutions and related best practices, and various standards bodies have projects underway, the issues of adoption and diffusion are predicated on understanding of the value proposition as it relates to an individual organization, industry segment, and society writ large.

NTIA could take a significant step towards understanding the factors that have influenced adoption and diffusion to date by designing a well-structured, multi-stakeholder engagement to clarify what actions have been taken, where those actions have been taken, the conclusions that have been reached, and the lessons learned from their implementation across multiple sectors. More importantly, such an inquiry could have the added benefit of providing further insight into potential synergies that result from collective action in engagement in these areas.

C. Cybersecurity and the Internet of Things (IoT)

The IoT presents society with an unparalleled level of cybersecurity issues, given its sustained exponential growth, and the diversity of stakeholders who will develop, market and use IoT-enabled devices and applications. In a 2015 report to the President’s National Security Telecommunications Advisory Committee (NSTAC), the authors noted that “the adoption of the IoT is creating a dramatic increase in the number of sensors and devices that can

³² See, Government Accountability Office Report, *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use*, GAO 12-92, December, 2011(available at: <http://www.gao.gov/assets/590/587529.pdf>) (visited May 21, 2015).

³³ See, *Request*, p. 14362, Sections 2 (b), (c).

autonomously communicate, thus creating massive new data sources and increasing automation that is often far removed from any human interaction. Potential benefits include the development of innovative services and, in many cases, more efficient use of infrastructure.

However, the security risks resulting from an exponential expansion in attack surfaces, a changing threat landscape, privacy concerns, an increased potential for kinetic-focused cyber-attacks, and changes to the hardware lifecycle must also be considered.”³⁴

What makes IoT particularly challenging from a cybersecurity perspective is that all of the factors that contribute to current vulnerabilities and concerns (e.g., accelerated market entry, cost reduction, insufficient security-by-design, and privacy) are increased by orders of magnitude. The question that NTIA raises in the Request is “how can we foster the emergence of voluntary policy frameworks, informed by market dynamics that enable IoT innovation while addressing the full spectrum of risks associated with cyber-physical systems?”³⁵

One of the primary goals of a policy framework for IoT should be to ensure that, while innovation remains unimpeded, security considerations and voluntary practices are incorporated into multiple dimensions of the risk landscape. This is especially the case given what is currently known about the IoT environment. In a recently released report by the E&Y consultancy, it is estimated that 70% of the most commonly used IoT devices contain vulnerabilities.³⁶ The authors state that these concerns are further exacerbated since “we cannot tell exactly what kind of threats will emerge next year, in five years’ time, or in 10 years’ time; we can only say that these threats will be even more dangerous than those of today.” Multiple

³⁴ See, DHS website, National Security Telecommunications Advisory Committee Report, *Industrial Internet Scoping Report*, February 19, 2014 (available at: https://www.dhs.gov/sites/default/files/publications/Final%20NSTAC%20Industrial%20Internet%20Scoping%20Report_0.pdf) (emphasis added) (visited May 21, 2015).

³⁵ See, *Request*, p. 14362, Section 2 (i).

³⁶ See, Ernst & Young Report, *Cybersecurity and the Internet of Things*, March, 2015 (available at: [http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/\\$FILE/EY-cybersecurity-and-the-internet-of-things.pdf](http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf)) (visited May 21, 2015).

institutions are currently working to apply frameworks and standards including NTIA's sister agency, the NIST.³⁷

Given the security implications, USTelecom members understand that security is essential for the growth of business and commerce in the IoT space. For this reason, they are working on crucial security standards in a variety of venues to ensure such measures are resident in any future IoT offerings. For example, many USTelecom members are active contributors in forums such as the Alliance for Telecommunications Industry Solutions (ATIS) and the Groupe Speciale Mobile Association (GSMA). Through their participation in such collaborative venues, industry is ensuring that robust security measures are developed and implemented on a standardized and global basis.

NTIA can play a crucial role in this area by promoting the use of the various solutions developed through organizations such as the ATIS and the GSMA throughout broader industry segments. For example, the Department could promote use of such solutions by highlighting some specific use cases around various IoT industries such as automotive, healthcare information technology, utilities and others. By highlighting these approaches, the Department can better facilitate industry taking proactive measures to stay in front of these issues.

NTIA must also ensure that any policy framework it implements is sufficiently flexible to accommodate new information related to evolving market dynamics, stakeholder resource concerns and business models, infrastructure and operating environments, end-user expectations and awareness, and laws and regulations. It will be equally important for NTIA to consider and implement international developments and perspectives as well. NTIA should

³⁷ See, NIST Preliminary Discussion Draft, *Framework for Cyber-Physical Systems*, Release 0.7, March 3, 2015 (available at: http://www.kslaw.com/library/newsletters/dataprivacysecurity/2015/0316/dps031615_preliminarydiscussiondraft.pdf) (visited May 21, 2015).

begin the development of its policy framework with a set of consensus-based principles that could help guide the identification and formulation of appropriate policy considerations.

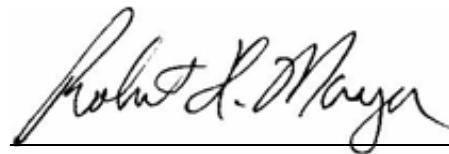
VII. Conclusion

All of the challenges discussed in these comments require further collaboration among all key stakeholders who share responsibility for protecting themselves and their customers from pernicious cyber threats. NTIA can build upon the work that has been completed and is currently underway by carving out stakeholder-defined initiatives, in any of these areas, to promote education, awareness and voluntary practices across the broad stakeholder community. An NTIA-facilitated effort that brings key players to the table to evaluate the current state of affairs, the lessons that can be learned from previous and current experiences and the identification of processes that are most likely to have an impact on reducing current and evolving threats should be supported by all ecosystem stakeholders.

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION

By:



Robert Mayer
Kevin G. Rupy

Its Attorneys
607 14th Street, NW, Suite 400
Washington, DC 20005
(202) 326-7300

May 27, 2015