September 26th 2014

Mr. Jeffery Goldthorp
Associate Bureau Chief for Cybersecurity and Communications Reliability
Federal Communications Commission
445 12th St., NW
Washington, D.C. 20554
jeffery.goldthorp@fcc.gov

Dear Jeff,

CTIA respectfully submits the attached comments regarding the Public Safety and Homeland Security Bureau's request for comment on implementation of CSRIC III Cybersecurity Best Practices, dated July 25th, 2014 (DA 14-1066). The comments represent the efforts of CTIA's Cybersecurity Working Group (CSWG) which is comprised of industry experts in the field of mobile cybersecurity.

Should there be any questions regarding the comments provided or clarification needed, please do not hesitate to let us know.

Yours truly,

/Scott Bergmann/

Scott Bergmann
Vice President Regulatory Affairs

/John A. Marinho/

John A. Marinho
Vice President, Technology and Cybersecurity

Copy to:
Ms. Lauren Kravetz
Deputy Chief of the Bureau's Cybersecurity and Communications Reliability Division
lauren.kravetz@fcc.gov

CTIA–The Wireless Association
Cybersecurity Working Group (CSWG)

Comments to
The Federal Communications Commission's
Public Safety and Homeland Security Bureau
on
Public Notice, FCC's Public Safety and Homeland Security Bureau Requests Comment on Implementation of CSRIC III Cybersecurity Best Practices, DA 14-1066 (July 25, 2014)

Submitted September 26, 2014

TABLE OF CONTENTS

I. INTRODUCTION AND EXECUTIVE SUMMARY

As policymakers have been grappling with cybersecurity, the Federal Communications Commission ("FCC") has been engaged with the private sector. The Communications Security, Reliability and Interoperability Council ("CSRIC") plays a central role in cybersecurity at the FCC, providing recommendations to the Commission and bringing industry together to address technology and policy issues. The FCC's Public Safety and Homeland Security Bureau ("Bureau") issued a Public Notice seeking comment from ISPs, the Internet community, consumer organizations, and the public on certain CSRIC III recommendations and alternatives developed since CSRIC issued these recommendations.

The Public Notice asks for input on implementing recommendations from CSRIC III regarding: (1) securing the Domain Name System (DNS) through DNSSEC,[1] (2) strengthening the inter-domain routing infrastructure through Secure Border Gateway Protocol extensions (BGPSEC),[2] (3) implementing source-address filtering with identified best current practices,[3] and (4) the Anti-Bot Code of Conduct to address distributed denial of service (DDoS) attacks.[4]

---

[1] *See* Public Notice, FCC's Public Safety and Homeland Security Bureau Requests Comment on Implementation of CSRIC III Cybersecurity Best Practices, DA 14-1066, at 1 n.2 (July 25, 2014) ("PN" or "Public Notice") (citing CSRIC III Working Group 5 DNSSEC Implementation Practices for ISPs: Final Report (Mar. 2012), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG5-Final-Report.pdf ("CSRIC III WG 5 2012 DNSSEC Final Report")).

[2] *Id.* (citing CSRIC III Working Group 6 Secure BGP Deployment: Final Report (Mar. 2013), *available at* http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_%202013.pdf ("CSRIC III WG 6 Final Report")).

[3] *See id.* at 1, nn. 6–8 (citing BCP 38/RFC 2827, BCP 84/RFC 3704, and CSRIC III Working Group 4 Final Report: BGP Security Best Practices (Mar. 2013), *available at* http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf ("CSRIC III WG 4 Final Report—BGP Security Best Practices")).

[4] *See id.* at 1, n.2 (citing CSRIC III Working Group 7 Final Report: U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs) (Mar. 2012), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf ("CSRIC III WG 7 Final Report—Anti-Bot Code")).

CTIA appreciates the attention that the FCC and Bureau bring to cybersecurity in the communications sector. The communications sector, including the wireless ecosystem, has been refining best practices and innovating in cybersecurity, and is actively participating in CSRIC IV activities looking at these issues. CTIA encourages the FCC to continue to support truly voluntary, industry-led efforts, as envisioned in the President's Executive Order on Critical Infrastructure Cybersecurity.[5]

As described in Part II of these comments, the wireless and tech industries are leading the way on cybersecurity and are being effective; for example, the U.S. mobile smartphone malware infection rate is one of the lowest in the world, at less than two percent. Industry is actively engaged through multiple public-private partnerships in the U.S., and through international standards-setting bodies. Cybersecurity threats are not limited to ISPs, but affect the entire Internet ecosystem. No one actor or segment can act alone to mitigate these threats; instead, all parts of the ecosystem must work together.

As explained in Part III of these comments, CSRIC avoids a one-size fits all approach and is free from mandates or regulatory burdens; this is why it works. The continued success of this model is key to the implementation of a regulatory paradigm that uses CSRIC and other voluntary public-private partnerships to advance use of the NIST Framework in a fashion that is flexible and adapts to the changing threat landscape. Diverging from CSRIC's longstanding voluntary, collaborative approach would change expectations surrounding CSRIC and threatens to divert attention and slow momentum on activities related to security. CSRIC IV has been tasked with updating many past CSRIC recommendations and aligning them with the NIST

[5] *See* Exec. Order No. 13636 – Improving Critical Infrastructure Cybersecurity § 8 (Feb. 12, 2013) (creating a "voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities"), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Framework released in February of 2014; therefore, reporting or accountability based on these past recommendations would be backward-looking and counterproductive. CTIA appreciates the FCC's continued commitment to the CSRIC model and process as the critical venue for considering issues related to the implementation and refinement of CSRIC recommendations.

The CSRIC process has been effective. As explained in Part IV, industry has been leveraging earlier CSRIC recommendations on a voluntary basis as appropriate for each organization. The recommendations have been helpful, but they have notable limitations: CSRIC III's was not focused on wireless; some threats identified in the Public Notice are not critical problems in the current mobile landscape, and success depends on further innovation and ubiquitous deployment of solutions by all contributors to the global Internet and wireless ecosystems. Given these issues, it would not make sense to expect or demand the wholesale adoption of the recommendations put forward by CSRIC III.

CTIA welcomes the FCC becoming even more engaged in cybersecurity activities. However, given the many activities underway in CSRIC IV and other venues, including at the National Institute for Standards and Technology ("NIST"), it is surprising that the FCC would ask for substantial input into these topics through this Public Notice. FCC officials have called for a "new regulatory paradigm" in which industry must "step up" to the FCC's satisfaction or face yet-unspecified regulation.[6] The private sector takes seriously its role in security and works with numerous government agencies on security in various partnerships to help deliver better and

[6] *See, e.g.*, Remarks of FCC Chairman Tom Wheeler to the American Enterprise Institute (June 12, 2014) ("[T]he network ecosystem must step up to assume new responsibility and market accountability for managing cyber risks" and the FCC will look the market while "preserving other options if that approach is unsuccessful."), *available at* http://www.fcc.gov/document/chairman-wheeler-american-enterprise-institute-washington-dc; July 29, 2014 Letter from Chairman Wheeler to Chairman Rogers (stating that the FCC expects industry to meet its expectation so that "prescriptive regulation is not necessary"), *available at* http://www.fcc.gov/document/chairman-response-regarding-cybersecurity.

safer solutions to consumers. The FCC has a seat at the table and, through those venues, a great deal of information and perspective is available.

CTIA urges the FCC to avoid regulation in this space and allow existing voluntary and collaborative efforts to continue, preserving the Commission's long standing, light touch in the areas of Internet and wireless policy. The private sector relies upon the Administration's assurance that its current cyber policy centers on truly *voluntary* action. As explained in Part V, regulation cannot keep pace with technological innovation, and attempts to impose regulation in this sphere could result in an innovation slow-down and hinder the industry's ability to respond to the dynamic and very fast-paced threat environment. Reporting or public assurance obligations would be *de facto* regulation and are ill-advised, and in any event, incentives are not aligned today for optimal information-sharing.

There remains much the Commission can do to improve our nation's cybersecurity. The FCC should continue to foster cooperation with the private sector through CSRIC and the NIST Framework process, support industry efforts to improve security throughout the global ecosystem, and work with Congress to create the kinds of information-sharing safeguards needed to fully protect shared information.

II. THE GLOBAL WIRELESS AND INTERNET INDUSTRIES ARE ADDRESSING SECURITY.

The wireless and tech industries are leading on security, which requires constant vigilance and innovation due to the rapid pace of change. CTIA's members prioritize security with monitoring, cutting-edge analysis, and investment in research and development of new solutions, all of which drive continued growth.

A. Cyber threats are constantly evolving.

The cyber threat profile is remarkably dynamic; "[c]ybercriminals continued to find new avenues to commit digital crime and evade countermeasures applied against their creations."[7] Malware is one example of evolving threats. "Online banking malware [has] continued to thrive with the emergence and/or modification of new malware families, each with different targets and varying anti-detection techniques."[8] Malware authors respond to the market. For example, the game Flappy Birds was released in 2013 with great success (over 50 million downloads). But according to a recent McAfee study, there are hundreds of clones of the game, and a vast majority of them are malicious malware.[9] Opportunists leverage current events to engage in phishing and probe attempts, and they harness news of cyberattacks and data breaches to exploit consumers through social engineering. The landscape of 2014 is not the same as in 2012, and it continues to evolve. Despite the evolving threats, the private sector is largely succeeding in protecting consumers and continually responding to ever-changing threats.

B. The wireless and tech industries lead on cybersecurity.

The communications sector is constantly investing in new methods and technology. Industry takes an active approach to sharing best practices and keeping abreast of the latest threats. From Internet Service Providers ("ISPs") and carriers to Operating System ("OS") developers, original equipment manufacturers ("OEMs"), and applications stores, the private sector is innovating, through proprietary research and development as well as commissioned scientific studies. Research is helping identify and refine threat indicators, technical

---

[7] TrendMicro, TrendLabs 1Q 2014 Security Roundup, *Cybercrime Hits the Unexpected: Bitcoin- and PoS-System Related Attacks Trouble Users*, at 9 (2014), *available at* http://about-threats.trendmicro.com/us/security-roundup/2014/1Q/cybercrime-hits-the-unexpected/.

[8] *Id.*

[9] McAffee, McAffee Labs Threats Report (June 2014), *available at* http://www.mcafee.com/common/js/asset_redirect.html?eid=14Q4GLOBALWBOSM1907&url=http:%2F%2Fwww.mcafee.com%2Fus%2Fresources%2Freports%2Frp-quarterly-threat-q1-2014.pdf.

improvements to network and communications infrastructure, and remediation and notification challenges. In addition to network operators providing security for communications transmission, OEMs, operators, and platforms promote a wealth of optional tools to improve security and data protection for information that resides on the smartphone or tablet. Beyond the technical and service innovation, the ecosystem shares information about threats and responses.

Illustrating industry's activity, CTIA has released five White Papers addressing cybersecurity in the last few years, the most recent in September 2014. These White Papers draw from member experience and research on varied topics, describing industry trends in mobile usage and cyber threats, analyzing cybersecurity and the Internet of things, and offering current best practices. CTIA's most recent White Paper, Today's Mobile Cybersecurity: Information Sharing, highlights the need for legislation to permit more information-sharing between ecosystem players and the government, as discussed in Section V below.[10] Industry participants also undertake extensive research, and release their own papers and analyses.[11]

These and other industry efforts promote innovation and experimentation. As a result, varied solutions are available. In addition to network operators providing security for communications transmission, network operators and platforms promote to enterprise and individual consumers a wealth of proprietary services and tools that can improve security, and consumers have options to protect information that resides on a smartphone or tablet.[12] Tools

---

[10] *See* CTIA, Today's Mobile Cybersecurity: Information Sharing (Sept. 9, 2014), *available at* http://www.ctia.org/docs/default-source/default-document-library/ctia_informationsharing.pdf ("Information Sharing White Paper").

[11] *See, e.g.*, Verizon 2014 Data Breach Investigations Report, *available at* http://www.verizonenterprise.com/DBIR/; Cisco Midyear 2014 Security Report, *available at* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000502656; Neustar Annual DDoS Attacks and Impact Report (2014), *available at* http://2014-annual-ddos-attacks-and-impact-report.pdf

[12] *See, e.g.*, Android Official Blog, *Expanding Google's Security Services for Android* (Apr. 10, 2014), *available at* http://officialandroid.blogspot.com/2014/04/expanding-googles-security-services-for.html; Apple, *iOS Security* (Feb. 2014), *available at* http://www.apple.com/ipad/business/docs/iOS_Security_Feb14.pdf; *Samsung*

include device management capabilities, anti-theft, anti-malware, browsing protection, app reputation checking, call/SMS blocking and scanning, and firewalls. Similar to how security needs are addressed in the physical environment and the desktop, network service operators, platforms, and device manufacturers provide consumers with a choice of security tools that empower them to protect their devices and their information. The industry's competitive environment works in favor of advancing cybersecurity because each player understands the advantages of marketing products and services that deploy security solutions consistent with consumer demand; this provides choice and diversity.

In addition to technical innovation, the ecosystem actively shares information about threats and responses. These efforts are not always public-facing, but extensive work is undertaken. As explained in CTIA's most recent white paper, "[t]oday's mobile cybersecurity is supported by a wide array of public-private forums," including the National Cybersecurity and Communications Integration Center ("NCCIC"), the Communications Information Sharing and Analysis Center ("Comm-ISAC"), the Communications Sector Coordination Council ("CSCC"), and the National Security Telecommunications Advisory Committee ("NSTAC").[13] These forums "make possible certain exchanges of information related to cybersecurity threats that can impact mobile communications."[14] These voluntary, collaborative processes are critical, particularly as industry evaluates and works through the NIST Framework.

Trisects Knox, Launches Entry-Level Free Version, zdnet.com (Sept. 18, 2014), *available at* http://www.zdnet.com/samsung-trisects-knox-launches-entry-level-free-version-7000033805/; Windows, *Microsoft Security Essentials*, *available at* http://windows.microsoft.com/en-us/windows/security-essentials-download; Blackberry, *There's Good Security and Then There's National Security: BlackBerry10 and BES10*, *available at* http://us.blackberry.com/content/dam/blackBerry/pdf/business/english/BlackBerry-Security-Brochure.pdf.

[13] *See* Information Sharing White Paper at 4.

[14] *Id*. at 13.

As a result of this vigilance and innovation, the United States is a leader in cybersecurity risk management. The U.S. mobile smartphone malware infection rate is less than two percent, which is one of the lowest in the world, and significantly lower than smartphone malware infection rates in Germany, Russia, and India.[15] Similarly, the United States is ranked second overall in "the ability to withstand cyber attacks and to deploy the digital infrastructure necessary for a productive and secure economy."[16] The U.S. communications sector is leading the way. But even though malware rates in the U.S. are comparatively low, industry is taking additional steps to improve security. This includes everything from improving app store management and offerings, to further experimenting with software and hardware solutions, and expanding user education.

C. All sectors of the global wireless ecosystem must work together to promote cybersecurity.

This leadership is working in large part due to the multilayered approach taken throughout the Internet and wireless ecosystem. Such an approach is needed because no one part of the communication sector or the mobile ecosystem—ISPs, carriers, OS developers, or manufacturers—can be the focus of security.

Contributors to the environment are diverse: large, small, domestic, international. And internet traffic—sources, destinations, and the points in between—respects no geographic limits. All participants share responsibility for cybersecurity and provide multilayered protection. At the input level, network-based security relies on network management and the trust built into global internet governance. Network-based security contributes to the overall security of the

---

[15] Mike Dano, *Report: U.S. Mobile Malware Infections Drop 63%*, FierceMobileIT (July 25, 2013), *available at* http://www.fiercemobileit.com/story/report-us-mobile-malware-infections-drop-63/2013-07-25.

[16] Booze Allen Hamilton, Cyber Power Index, *available at* http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf.

ecosystem and is one of the major reasons that botnets and malware are not prevalent on U.S. systems. At the mobile services level, data and email can be protected through encryption. At the downstream level, security solutions include end-user education, authentication, secure connectivity, and other device solutions. And third parties are entering the security space with enterprise solutions and consumer products and services.

As CSRIC reports noted, cybersecurity threats "impact the entire Internet ecosystem" and effective solutions "require collective action by all parts of that ecosystem, including end-users, software developers, search providers, websites, e-commerce sites, and others."[17] Notably, "end-user devices are outside of the control of ISPs" or any one actor, so all participants "need to work together" to improve security.[18] Likewise, in the context of Internet routing and domain name security, no single layer can control security. The "foundational system was built upon a distributed unauthenticated trust model," such that security improvements often require "global adoption and implementation" to be successful.[19]

This interdependence underscores the importance of collaboration. In addition to domestic activities of the sort identified above, international standards-setting organizations—like IETF, ATIS, Committee T1, 3GPP, and the IEEE—demonstrate ongoing commitment to advance the state of the art for cybersecurity. These organizations are in the process of addressing internet and mobile security.

For example, the Third Generation Partnership Project ("3GPP") is working with GSMA to develop a certification program for 3GPP's Security Assurance Methodology ("SECAM") program to help secure mobile network architectures. 3GPP has produced the SECAM—a

---

17 CSRIC III WG 7 Final Report- Anti-Bot Code, at 10.

18 *Id.*

19 CSRIC III WG 4 Final Report - BGP Security Best Practices, at 8; *see also* CSRIC III, WG 4, *Final Report - DNS Best Practices,* at 8 (Sept. 2012) ("CRIS III WG 4 Final Report - DNS Best Practices").

technical report describing a new security assurance and evolution framework for mobile network products. This framework aims to provide common and testable baseline security properties for the different network product classes.[20] It will provide specifications for each network product class, to cover the assets, threats, and security objectives. It will include detailed functional requirements and assurance or test cases, and have details for basic vulnerability testing, *e.g.*, vulnerability scanning tests, DoS testing, and protocol fuzzing. Other standards groups are looking at varied elements of network and Internet security, including efforts to refine mature standards for Resource Public Key Infrastructure ("RPKI") in BGP routing. There is a lot of activity underway at all levels of the ecosystem.

III. THE PUBLIC NOTICE FOCUSES ON EARLIER, VOLUNTARY RECOMMENDATIONS FROM CSRIC III, WHICH ARE CURRENTLY BEING EVALUATED.

A. Communications security was part of CSRIC III and CSRIC IV.

CSRIC III's purpose was to "provide recommendations to the FCC regarding ways it can strive for security, reliability, and interoperability of communications systems . . . including . . . the reliability and security of communications systems and infrastructure."[21] CSRIC III was tasked with making recommendations, among other things, to prevent cyber threats, facilitate rapid restoration of communications in widespread outages, and help secure end-users and

[20] The SECAM framework includes agreement on the relevant threat model and needed assurance level; definitions of the process to build the SeCurity Assurance Specifications ("SCAS"), which will contain the security requirements for a network product class and the associated test cases; and descriptions of the roles and process needed for security assurance, evaluation, and accreditation.

[21] *Id.* CSRIC III took place from March 19, 2011 to March 18, 2013.

servers.[22] Several working groups addressed cybersecurity, including DNS security and DDoS threats, as well as inter-domain routing issues and BGP.[23]

Members of CSRIC III devoted enormous resources to identify, develop, refine and finalize these many reports and recommendations, with the goal of providing a valuable resource to industry and the FCC for consideration and voluntary use. As appropriate, individual companies' "opt-in" could support future, "incremental" development of some or all of the ideas put forth.[24] In some cases, the reports explicitly noted that the views expressed are "not necessarily shared by all of the working group members" and pointed out that the groups are "strictly *advisory* in nature" and were simply providing recommendations that "encourage the market-led adoption of security technologies rather than advocating any regulatory policy or inventing any new security solutions."[25] Many of the reports called for additional research, review, and refinement in future CSRIC efforts. Those efforts are underway.

CSRIC IV's goal is similar in many respects to that of CSRIC III's goals. It intends to "provide recommendations to the FCC regarding ways it can strive for security, reliability, and interoperability of communications systems . . . including [on] the reliability and security of

---

[22] *See* CSRIC III Working Group Descriptions and Leadership (Nov. 15, 2012), *available at* http://transition.fcc.gov/pshs/advisory/csric3/wg-descriptions.pdf ("CSRIC III Working Group Descriptions").

[23] CSRIC III's Working Groups reports address these issues. *See* CSRIC III WG 4 Final Report – DNS Best Practices; CSRIC III WG 4 Final Report—BGP Security Best Practices; CSRIC III WG 5 2012 *DNSSEC Final Report*; CSRIC III, WG 5, *Final Report on Measurement of DNSSEC Deployment* (Feb. 2013) ("CSRIC III WG 5 DNSSEC Deployment Final Report"); CSRIC III WG 6 Final Report; CSRIC III WG 7 Final Report—Anti-Bot Code; CSRIC III, WG7, *Final Report - Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs) Barrier and Metric Considerations* (Mar. 2013); CSRIC III, WG 11, *Final Report - Consensus Cyber Security Controls* (Mar. 2013).

[24] CSRIC III WG 6 Final Report, at 2.

[25] *Id.* at 3 (emphasis in original). Similarly, Working Group 7 noted that "participation is voluntary and [the Code] encourages types of actions to be taken by ISPs, however this Code does not require any particular activity. CSRIC III WG 7 Final Report—Final Anti-Bot Code, at 11.

communications systems and infrastructure, particularly mobile systems."[26] In particular, CSRIC IV's Working Groups are tasked with the following:

- Working Group 4's revised mission is to "develop 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. The macro-level assurance will demonstrate how communications providers are reducing cybersecurity risks through the application of the NIST Cybersecurity Framework, or an equivalent construct."[27]

- Working Group 5 is "examin[ing] and mak[ing] recommendations to the Council regarding network level best practices and other measures to mitigate the effects of DDoS attacks from large data centers and hosting sites."[28]

- Working Group 6's DNS Subgroup aims to "identify and plan for long-term remedies to DNS vulnerabilities."[29] This group also is actively engaging on inter-domain routing issues.

The CSRIC IV Working Groups' efforts have been in progress for over a year, and, like CSRIC III, are premised on voluntary industry collaboration that yields consensus recommendations for individual companies to evaluate and consider.

B. The Public Notice appears to start down a path toward backward-looking "self-regulation" requiring compliance with particular standards.

The PN states that industry has "not yet provided" the government with "sufficient" information to help the FCC assess the implementation of certain CSRIC III "recommendations."[30] When considered with other statements about the need for a new

---

[26] CSRIC IV began on March 19, 2013 and will end two years from that date, in 2015. *See* Charter of the FCC's Communications Security, Reliability, and Interoperability Council, *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC%20Charter%20Renewal%202013.pdf ("CSRIC IV Charter).

[27] CSRIC IV Working Group Descriptions and Leadership, at 5 (Sept. 2, 2014), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_IV_Working_Group_Descriptions_9_2_14.pdf. CSRIC Working Group 4's description was originally focused on harmonizing updated cybersecurity best practices with the NIST Framework. In early September 2014, a year and a half into CSRIC IV's term, the FCC altered the description to incorporate an oversight role.

[28] *Id.*

[29] *Id.* at 6.

[30] Public Notice at 1.

regulatory paradigm and assurances from industry, this appears to start the FCC down a path toward *de facto* regulation," in the form of an accountable or enforceable "checklist" approach that, practically speaking, converts voluntary industry practices into required "self-regulation." CTIA has serious concerns about such an approach. The success of CSRIC largely is due to it being viewed as a non-regulatory exercise where engineers, policy experts, and other subject matter experts could openly discuss common practices to address cybersecurity threats.

First, a more regulatory approach would fundamentally alter CSRIC's role. CSRIC presently is seen as an open and transparent venue, in which industry works with the FCC at a technical level on cybersecurity solutions that offer the necessary flexibility for businesses to appropriately adjust to threats. Treating its recommendations as *de facto* requirements or a foundation for future Commission action would mean that all proposals advanced via CSRIC would have to be viewed as platforms for oversight and future federal mandates. This could fundamentally undermine the past dynamic at CSRIC, and create a new model in which recommendations, voluntary or otherwise, must be seen as precursors to future regulation. This could have a chilling effect on the collaborative spirit upon which the CSRIC relies to achieve outcomes supported by both the Commission and industry. Effectively addressing cybersecurity calls for a functioning public-private partnership. Post-hoc attempts by the Commission to validate or test the use of "voluntary" practices threatens to diminish the benefits of that working relationship.

Second, industry is skeptical of any approach that results in a rigid checklist or specific standards. This model promises to be ineffective, and it could be harmful, undermining security by pushing industry toward a narrowed approach that could quickly become outdated and to which limited resources would flow instead of the development of new solutions. Worse, it can

provide a more focused target for attackers. Industry supports appropriate security standards and participates in forums like NIST and CSRIC, which enable the private sector to work on common approaches. These efforts can, in turn, feed into international efforts. But industry must have flexibility to address changing threats. Adhering strictly to one- or two-year-old recommended practices could needlessly put consumers at risk. Operators need to continually update their practices to meet evolving threats to networks.

Third, the challenges identified by the PN have a broad, global impact. They simply cannot be addressed by ISPs—or any one part of the ecosystem—alone. Effective cybersecurity requires a comprehensive approach. The botnet code of conduct, implementation of DNSSEC, and improving BGP security are shared responsibilities that require action by multiple sectors, including the Information Technology ("IT") sector.

CSRIC IV is working from and in many cases updating the work of CSRIC III, because addressing cyber issues is an evolving process. Indeed, many of CSRIC IV's explicit charges are to update or expand earlier CSRIC work: Working Group 6/Inter-Domain Routing Subgroup has been asked to review recent Internet route hijacking incidents and review the CSRIC III recommendations to determine if updates are needed. Working Group 6/Inter-Domain Routing Subgroup has also been asked to Recommend three categories of best practices or standards (*e.g.*, from CSRIC III Working Group 4 or IETF) for which a detailed implementation plan will be developed by the end of CSRIC IV. The recommendations could include, for example, Secure Border Gateway Protocol ("BGPSEC") or DNSSEC, addressed in CSRIC III. CSRIC IV will update or overtake some items addressed in CSRIC III. Indeed, CSRIC IV specifically

recognizes that "[i]n the time that has passed, cybersecurity threats have become more pronounced and visible, and our nation's cybersecurity policy has evolved."[31]

A notable new aspect of the work of CSRIC IV and industry involves the NIST Framework released earlier this year. Where CSRIC III's recommendations and reports reflected a strategy focused on providing a compendium of best practices tied to a set of threat assumptions that existed 3 years ago, the NIST Framework is a voluntary, risk-based strategy that is designed to adapt and foster innovation in response to a changing threat landscape. Industry has been supportive of the Framework, welcoming the effective, collaborative, and iterative approach NIST has used. It requires careful consideration to assess how it can best assist the communications sector. That consideration is underway.[32] Industry is already hard at work mapping existing best practices and standards to the Functions, Categories and Subcategories identified in the Framework. Every part of the global ecosystem should have a chance to consider whether and how the Framework, or a similar construct, can help their organization evaluate and improve their cybersecurity.

In light of this ongoing collaborative, complementary activity, the Public Notice's request for information to promote accountability for CSRIC III recommendations and best practices may not be the most productive use of resources, particularly while CSRIC IV is pursuing

---

[31] *Id.* In addition, the Public Notice requests industry information on CSRIC III's ABCs for ISPs Report, which relates to Working Group 5's current work. Working Group 5 has specifically addressed the evolving botnet threat, stating that "[t]he botnet architecture is becoming more sophisticated and difficult to trace and C2 command and control systems are increasingly tiered using proxy servers and peer to peer networking to obfuscate the location of the system that is executing the commands. Additionally, some botnets have the ability to impair a compromised system after it has completed an attack." CSRIC IV, Working Group 5 Remediation of Server-Based DDoS Attacks, Interim Report, 15 (June 18, 2014), *available at* http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-5_Report_061814.pdf. Likewise, the Public Notice requests information regarding CSRIC III's recommendations regarding domain name security. CSRIC IV's Working Group 6 is currently addressing more current DNS vulnerabilities. The Public Notice also requests information on CSRIC III's recommendations regarding internet route hijacking. CSRIC IV's Working Group 6 is charged with "review of recent Internet route hijacking incidents and review of CSRIC III recommendations to determine if updates are needed."

[32] CSRIC IV Working Group Descriptions and Leadership at 5.

similar topics. More worrisome, the Public Notice seems to portend further public proceedings related to existing and developing voluntary efforts. Such a shift would be unfortunate. Turning earlier, voluntary solutions into *de facto* obligations or benchmarks is backward-looking and counterproductive. In many respects the cybersecurity conversation has moved on and expanded, as the FCC knows through the ongoing work of CSRIC IV. As explained below, the FCC can best effectuate its interests by supporting existing, effective approaches that productively harness private sector activity.

IV. INDUSTRY HAS BEEN USING AND BUILDING ON THE RECOMMENDATIONS MADE BY CSRIC III, AS APPROPRIATE, TO BETTER SECURE THE COMMUNCIATIONS SYSTEM FROM CYBER ATTACKS.

The Public Notice requests information regarding: (1) securing the DNS through the incremental implementation of DNSSEC; (2) strengthening the security of the Internet's inter-domain routing infrastructure; (3) source-address filtering to prevent attackers from spoofing IP addresses to launch DDoS attacks, with two best current practices; and (4) implementing the Anti-Bot Code of Conduct to mitigate the proliferation of DDoS attacks. While industry has been leveraging these CSRIC III recommendations on a voluntary basis as appropriate for each organization, it is important to recognize that these recommendations have inherent limitations as models for ecosystem security assessment. The FCC should encourage further consideration in current and future CSRIC efforts, and elsewhere, to keep pace with evolving technology and threats.

First, the CSRIC III recommendations at issue here generally did not include much consideration of wireless-specific issues or challenges. For example, the recommendations to secure the BGP are not directly applicable to wireless; BGP security issues can affect mobile device connectivity, but do not permeate into the cellular network. Similarly, the source address filtering BCPs recommended by Working Group 4 are not necessarily relevant to wireless.

CSRIC IV is addressing many of these issues with the additional perspective of wireless, as part of the long-term goal of improving the security of the ecosystem through incremental, systemic improvements.

Second, the threat profile in the communications sector has evolved. Many of the threats that the Public Notice focuses on, such as DDoS attacks and botnets, are not the most critical, particularly for wireless.[33] CTIA's Mobile Threat Report compiles a variety of threat-related reports to keep industry updated on mobile-related threat trends. While botnets are a serious concern, they are not currently a major mobile threat, as mobile networks do not have the power and bandwidth that residential and enterprise networks have for botnets to be effective.[34] Nevertheless, while it is rare that customers' mobile devices become infected with malware and generate traffic from the mobile network onto the Internet, the wireless industry is vigilant and is proactively looking ahead to mitigate this or similar threats in the mobile space in the future. Thus, DDoS attacks and botnets are part, but not all, of the story.

Third, the utility of many CSRIC III recommendations is further limited by a need for ubiquity in deployment. Because the threats identified by CSRIC III and the PN are not U.S. ISP-specific, U.S. ISPs are only one component of a broader ecosystem challenge. DNSSEC depends upon a variety of actions outside of ISP controls, such as domain owners signing their domains. Likewise, BGP/RPKI depends upon a range of actions through the chain including by Internet registries. Ubiquitous deployment can only be achieved through consensus and outreach, not regulation or post-hoc accountability efforts.

---

[33] As an example, BCP 38—one of the source-address filtering BCPs recommended by Working Group 4—is focused on defeating DDoS attacks which employ IP Source Address Spoofing. Furthermore, Working Group 7's Anti-Bot Code is singularly focused on mitigating the botnet threat in the wireline broadband space, and as described in the Code, "[b]ots are frequently used as part of coordinated Distributed Denial of Service (DDoS) attacks for criminal, political, or other motivations." CSRIC III WG 7 Final Report-Anti-Bot Code, at 8.

[34] For example, the widely-publicized Gameover Zeus botnet—which intercepted online banking transactions—was not a mobile-specific malware threat.

A. CSRIC III's recommendation to secure the DNS through DNSSEC requires broader action, making full adoption challenging.

CSRIC III's Working Group 5 was focused on steps to help protect against domain name fraud. In particular, it recommended various steps to secure the DNS.[35] First, CSRIC III recommended that ISPs implement their DNS recursive nameservers so that they are DNSSEC-aware. Second, CSRIC III urged key industry segments—like banking and healthcare—to sign their domain names. Third, CSRIC III recommended that software developers study how and when to incorporate DNSSEC validation functions into their software. Broadly, "the Working Group's task was to determine the pros and cons of ISP adoption of DNSSEC and recommend how ISPs might best achieve this task."[36]

While industry is implementing these recommendations as appropriate, the CSRIC III DNSSEC recommendations have limitations. DNSSEC was first proposed in 1997,[37] and since that time, the Internet and the threat landscape have changed dramatically.

As is the case with many of the recommendations highlighted in this PN, another limitation of the DNSSEC recommendations is that DNSSEC depends on ubiquitous deployment in the Internet hierarchy, which is at present unrealistic. The viability of DNSSEC is dependent upon a wide variety of actions outside of ISPs' control, such as domain owners signing their domains. However, the overwhelming majority of domains are not signed today. Indeed, we understand that the majority of U.S. government domains remain unsigned[38] despite the fact that

---

35 CSRIC III CSRIC III WG 5 DNSSEC Deployment Final Report , at 4-5.

36 *Id.* at 5.

37 Domain Name System Security Extensions RFC 2065, IETF (proposed Jan. 1997), available at https://datatracker.ietf.org/doc/rfc2065/.

38 NIST Information Technology Laboratory, Advanced Network Technologies Division, *Estimating USG IPv6 & DNSSEC External Service Deployment Status, available at* http://fedv6-deployment.antd.nist.gov/cgi-bin/generate-gov.

the U.S. government has mandated that agencies sign their public facing domains.[39] Additionally, the proliferation of new top-level domains ("TLDs") increases the challenge of ensuring registrar signing. Only 428 of 638 TLDs are currently signed, with 165 of the 210 unsigned TLDs being assigned to countries.[40] Only 35% of country-code TLDs are currently signed.[41]

Ubiquitous deployment of DNSSEC would be complicated. DNS involves both forward lookup (fully qualified domain name to IP address) and reverse lookup (IP address to fully qualified domain name). Full deployment of DNSSEC infrastructure necessitates both, which places means organizations need to deploy DNSSEC on both the ISP and domain name registry. Likewise, DNSSEC requires validation, which is a user issue: browsers, operating systems, and apps need to be DNSSEC-aware and be able to validate credentials. Currently, browsers accept unsigned records and will continue to do so for backward compatibility. Even if ISPs broadly deployed DNSSEC, the validation step is key for the protocol to be effective, but the FCC cannot ensure this. In light of these dynamics, committing to general availability of DNSSEC, and the validation function in particular, across entire global networks may be premature.

DNSSEC may also have unintended consequences. For example, DNSSEC may exacerbate other types of attacks, namely DNS amplification DDoS attacks. CSRIC III recognizes this risk of DNSSEC as well.[42] Similarly, deploying DNSSEC may impact reliability

---

[39] Office of Mgmt. & Budget, Exec. Office of the President, OMB Memo No. M-08-23, Securing the Federal Government's Domain Name System Infrastructure (2008), available at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf (requiring agencies to deploy DNSSEC to the top level .gov domain).

[40] Charles Clancy, *Assessment of DNSSEC Deployment Ubiquity Among TLDs*, CTIA Cybersecurity Working Group Report (Aug. 2014).

[41] *Id.*

[42] CSRIC III, WG 5, Final Report – DNSSEC Implementation Practices for ISPs, 31 (Feb. 2013) ("There is controversy as to whether DNSSEC exacerbates amplified DDoS attacks.")

and cost of services, and there is a risk of negative subscriber experience due to false alarms. Additionally, turning on DNSSEC requires capacity additions to handle the large incremental traffic driven by DNSSEC communications, while support protocols necessary to effectively use DNSSEC to mitigate man-in-the-middle attacks such as DNS-based Authentication of Named Entities (DANE) are not natively supported in any desktop application. Therefore, while DNSSEC is useful, it may not be the best solution in all circumstances.

Industry is innovating to address DNS security and has developed proprietary alternatives to achieve similar goals. To thoroughly address the complex challenges facing the DNS, industry needs to maintain the flexibility to innovate.

B. CSRIC III's recommendations to strengthen the security of the Internet's inter-domain routing infrastructure are still being evaluated and require broad cooperation.

CSRIC III addressed methods to secure BGP deployment, with the goal of protecting against misrouting, whether accidental or malicious. Working Group 6 aimed to recommend a "framework" for "incremental adoption of secure routing procedures and protocols based on existing work in industry and research."[43] The Final Report on secure BGP deployment noted that its conclusions were not necessarily shared by all members, and emphasized that "the autonomy of individual network providers and Autonomous System operators is critically important."[44]

Some industry participants follow many of the recommendations of Working Group 6 as appropriate—including compliance with best current practices, maintenance of public, complete and up-to-date Internet Registry records, and active engagement in various collaborative efforts and global standards-bodies. Further adoption of many of the best current practices discussed in

[43] CSRIC III WG 6 Final Report, at 3.

[44] *Id.* at 5.

Working Group 6's final report is being evaluated and may be prudent.[45] However, other BGP security approaches are still in early stages. These solutions are working through international standards bodies and actors in the ecosystem are working on implementation. For example, the RPKI approach remains in its early stages of maturity and adoption. It has not been officially adopted by the IETF, and there are still questions as to its implementation and utility. On a similar note, there is no mature and widely-accepted standard for route attestation, which means that available standards have limited value.

Like DNSSEC, BGP solutions require ubiquity to be truly effective. As described above, the Internet is a global network, and even if all U.S. entities deployed BGPSEC, it would be ineffective against cyberterrorism, cyberwarfare, and cybercrime unless adopted globally. ISPs in the United States are only one component of a broader Internet ecosystem; all component actors—including internet registries who could potentially provide a database of published, valid routes in support of an RPKI solution that has yet to be implemented—must act to secure the inter-domain routing infrastructure.

What is more, even if U.S. ISPs demanded signatures for every route, there would still be complexities and vulnerabilities. BGPSEC is only effective if every route in an AS-path is signed, and any AS that does not support BGPSEC strips the signatures of its peers before passing them on. NIST currently reports that only 5% of routes visible within the United States are signed, and of those that are signed, 10% are invalid.[46] As a result, there would be no guarantee of the true source origin because there would be no way to verify the signature beyond the touch point.

---

[45] *See id.* at 11–13.

[46] NIST Information Technology Laboratory, Advanced Network Technologies Division, *Validation Results of Unique IPv4 Prefix/Origin Pairs Using Global RPKI*, *available at* http://www-x.antd.nist.gov/rpki-monitor/.

In sum, significant cost/benefit concerns remain relevant in BGPSEC deployment, particularly where the foundation has not been laid for successful use based on global deployment. But even as the solutions recommended by CSRIC III are in flux, industry is innovating. There are other ways to secure the border gateways, like designing and checking routing tables automatically rather than by hand. Emerging proprietary solutions are more discrete and focused, and seem likely to be more effective to secure border gateways. These solutions confirm the need to maintain industry flexibility.

C. CSRIC III's recommendations for source-address filtering were developed for a different environment and are challenged by increasingly global internet traffic flows.

CSRIC III's Working Group 4 made several recommendations regarding source-address filtering as a way to combat source-address spoofing. Source address spoofing lets cyber attackers facilitate denial of service attacks. Noting that "[t]he scope of Working Group 4 [wa]s to focus on currently deployed and available feature-sets and processes and not future or non-widely deployed protocol extensions,"[47] CSRIC III recommended that network operators should apply filtering, and it referenced two BCPs—IETF BCP38/RFC 2827 and BCP 84/RFC 3704—for "more detailed advice and treatment."[48] Industry agrees that source-address spoofing is a problem that needs to be addressed, and portions of the CSRIC III recommendations have been implemented across networks in an effort to combat the threat.

Nonetheless, the recommendations identified in the Public Notice were established in a different Internet environment. Source address filtering is less effective and makes less sense now than it did three years after CSRIC III made its recommendations, and ten years or more from the BCPs' publication. This is mainly because the Internet is becoming more and more

---

47 CSRIC III WG 4 Final Report—BGP Security Best Practices, at 3.

48 *Id.* at 20.

dispersed and less traffic traverses the United States. While significant amounts of inter-regional Internet traffic flows to or through the United States, significant volumes of traffic and capacity connect directly to hubs outside the United States., *e.g.*, from Africa and the Middle East to Europe, or within other regions.[49] For example, more than 80% of North African, Middle Eastern, and Sub-Saharan African international Internet bandwidth connects to hubs in Europe, while 86% of Latin American international Internet bandwidth connects to the United States. By contrast, about 40% of Asian international Internet bandwidth connects to the United States, versus 28% to Europe.[50] Thus, in spite of U.S. Internet companies having a significant percentage of users outside the United States (86%), just four global Internet companies based outside the United States serve more than 1.6 billion users on a monthly basis.[51]

The BCPs highlighted in the PN, while not obsolete, can be made more effective with additions that consider the changing threat landscape. Industry is working on a variety of techniques—both static and dynamic—to address the risk of spoofing IP addresses to launch DDoS attacks. Such techniques leverage a multi-layered approach based on network monitoring, anomalous events, and other approaches that depend on network configuration, situational awareness, and risk profile. Industry needs to maintain flexibility to innovate and implement filtering techniques based on threats and risks; in some circumstances, those techniques will be closer to the static ingress filtering envisioned by the BCPs, but in other

---

[49] *See, e.g.*, Todd Lindeman, "A Connected World," The Wash. Post (July 6, 2013), *available at* http://apps.washingtonpost.com/g/page/business/a-connected-world/305/.

[50] *Id.; see also Asia's connectivity patterns shift as carriers become less dependent on US*, TeleGeography, (Oct. 17, 2013) *available at* http://www.telegeography.com/products/commsupdate/articles/2013/10/17/asias-connectivity-patterns-shift-as-carriers-become-less-dependent-on-us/; TeleGeography, *Global Internet Geography*, Executive Summary, Figure 2 (2014) *available at* http://www.telegeography.com/page_attachments/products/website/research-services/global-internet-geography/0005/1382/GIG_Executive_Summary.pdf.

[51] *See* Mary Meeker, *Internet Trends 2014 – Code Conference*, Kleiner Perkins Caufield Byers, at 131 (May 28, 2014) (citing comScore), *available at* http://s3.amazonaws.com/kpcbweb/files/85/Internet_Trends_2014_vFINAL_-_05_28_14-_PDF.pdf?1401286773

circumstances, industry will take advantage of dynamic ingress filtering, which is often more effective in mitigating DDoS attacks.

Even though source-address filtering does not necessarily require ubiquity, successful filtering requires action by more than one player. For example, dynamic filtering is often achieved through collaboration with outside security vendors. For source address filtering to be effective, players beyond the wireless industry must be engaged.

D. CSRIC III's Anti-Bot Code of Conduct has been useful and is being used as appropriate, though challenges remain.

CSRIC III's Working Group 7 developed a voluntary code of conduct for ISPs to address botnets, focusing on education, detection, end-user notification, remediation, and collaboration. The Code was targeted at ISPs offering residential broadband services, but the Code's recommendations only tell part of the story. Indeed, as the Report itself noted, its recommendations are meant to coexist with other efforts by many stakeholders in the ecosystem.[52] While many in industry are taking meaningful action on the recommendations, other entities in the ecosystem in addition to ISPs need to address the botnet threat.

As explained, while botnets are not a current major threat in mobility, the wireless industry is looking ahead to mitigate the *potential* for this kind of attack—or actions that imitate the symptoms of botnet attacks. Some of the CSRIC III's recommendations present challenges to this effort, particularly for mobile. For example, notification issues are complex, particularly in mobile. Given the opportunities for spoofing, the risk of consumer confusion, and other challenges, more thought needs to be given to how to effectively approach notification.

---

[52] CSRIC III WG 7 Final Report—Anti-Bot Code, at 12 ; *see also id.* at 10 ("It should be recognized that bots impact the entire Internet ecosystem and that successfully curtailing bots or mitigating their impact will require collective action by all parts of that ecosystem, including end-users, software developers, search providers, websites, e-commerce sites, and others. End-user devices are outside of the control of ISPs hence all participants in the Internet ecosystem need to work together to address this issue.").

Remediation is also complex. In the mobile environment, there are over six varieties of operating systems, a greater diversity of hardware platforms (*e.g.* smartphone, tablet, phablet, PCs), and a variety of ecosystem players (*e.g.* App Stores, OTT players that deliver services) and services unique to wireless (*e.g.* WEA, WPS, E911). Additionally, botnet remediation continues to depend on the changing threat landscape. For example, server-based botnets are more prevalent today than PC-based botnets, and they are virtually non-existent in the mobile environment. A variety of remediation tools are available from ISPs and carriers, as well as third parties. Indeed, given market demand as awareness and empowerment in security grow, the wireless industry expects more such tools to emerge and to be adopted.[53] As with the other areas, it is important that innovation is encouraged.

In sum, the CSRIC III recommendations identified in PN were useful. They identified best practices and steps that, as appropriate, could improve security. It would not make sense to take a backward-looking approach by seeking to hold stakeholders "accountable" for voluntary commitments made years ago, particularly where CSRIC IV is underway. Indeed, as described above, many of the recommendations are not addressed in today's environment and require globally ubiquitous adoption to be effective. Given that such an outcome is unrealistic, it would not make sense to require wholesale adoption of the recommendations.

---

[53] For example, the Online Trust Alliance issued a botnet remediation paper in 2013. *See* Botnet Remediation Overview & Practices, Online Trust Alliance (Oct. 1, 2013), available at https://otalliance.org/system/files/files/best-practices/documents/ota_2013_botnet_remediation_best_practices.pdf. Even though this industry alternative to the Anti-Bot Code of Conduct focuses on traditional computing devices, the report emphasizes that "future documents and updates will focus on the mobile landscape, recognizing that tablets, smart phones and similar mobile devices are outpacing the growth of PCs and increasingly being targeted by cyber criminals." *Id.* at 3.

V. THE FCC SHOULD PROCEED WITH CAUTION ON CYBERSECURITY, AND AVOID CREATING BURDENS THAT COULD SLOW INNOVATION AND COLLABORATION.

When it comes to cybersecurity, policymakers must balance complex policy and technical dynamics that, taken together, favor a very light touch from regulators. Cybersecurity is marked by complicated technical issues and rapid innovation, both with respect to the changing nature of the problem and solutions. Even if FCC oversight or regulation could keep pace, a federal regulatory role is destined to be inadequate because of the global and distributed nature of the challenges and solutions. The FCC should not seek post-hoc accountability for best practices and recommendations that were intended to evolve and to be used on a voluntary basis, as appropriate. Industry is working through domestic and international groups and standards bodies to develop and refine solutions. Those ongoing voluntary efforts should be supported.

A. Cybersecurity, Internet and mobile practices are poor candidates for regulation or agency oversight.

Wireless providers, wired ISPs, and other entities in the ecosystem require flexibility to be innovative in response to cyber threats. Given the rapid pace of innovation, the sensitivity of information about threats and capabilities, and the risks inherent in sharing information, cybersecurity, Internet and mobile practices are poor candidates for regulation, reporting mandates, or additional obligations. The Commission should avoid regulating network operator cybersecurity. It should think carefully about whether "assurance" requirements will be effective or counterproductive. And it should recognize the risks that currently attend the sharing of information.

1. Cybersecurity is not suited for prescriptive regulation.

Cybersecurity is not a good candidate for federal regulation, for several reasons. The time and compromises inevitable in agency efforts to set government standards virtually ensure

the obsolescence of any standards once adopted. This is particularly true where technology must move at a breakneck pace to keep up with ever-changing threats and techniques. Regulation will not facilitate nimble, rapid response and development of new cyber security measures. Indeed, regulation or standard-selection may thwart the innovation needed to stay ahead of malefactors who tailor attacks to evade solutions in near real-time.[54] Economics literature is full of regulatory efforts that "foreclosed innovation, selected 'incorrect' standards, or favored particular incumbent industries."[55] Formal standard-setting, either by government or by private parties, should be avoided during the time that the technologies in question are rapidly changing.[56] Proper federal regulation requires time, and is notoriously incapable of predicting technical needs and abilities, or keeping up with innovation. This would be especially true in the cybersecurity context, where creativity, speed, and responsiveness are required. Service providers and other commercial entities may be forced to direct resources towards abiding by government-preferred standards that may hamstring other, more effective initiatives.

Even if regulation were a useful model, existing cybersecurity recommendations, which properly are voluntary and flexible, do not provide a good regulatory foundation. Best practices and evolving industry approaches are far from the sort of binding standards that could be suitable models for federal regulation or incorporation by reference.[57] They were never designed for that purpose.

---

[54] *See* Promisec, *The Evolution of Cyber Threats: Hackers Target Mobile & Cloud* (Mar. 18, 2013), *available at* http://www.promisec.com/blog/the-evolution-of-cyber-threats-hackers-target-mobile-cloud/ ("Cyber criminals and APTs are becoming more sophisticated faster than anti-virus providers can keep up.").

[55] *See, e.g.*, Comment of Michael G. Baumann & John M. Gale, *Video Device Competition*, MB Docket No. 10-91 (July 19, 2010) (titled "Economic Analysis of the Regulation of MVPD Navigation Devices"), *available at* http://www.ei.com/downloadables/mgb_report.pdf.

[56] *See, e.g.*, Stanley Besen and Leland Johnson, *Compatibility Standards, Competition, and Innovation in the Broadcasting Industry*, Rand, ix (Nov. 1986).

[57] *See, e.g.*, Emily S. Bremer, *Incorporation by Reference in an Open-Government Age*, 36 Harv. J.L. & Pub. Pol'y 131, 202 (2013) (noting that under federal policy requiring agencies to avoid government-unique standards

Even if those limitations could be overcome, any Commission approach will focus on entities within the FCC's jurisdiction here in the United States. But, any such effort is destined to be inadequate in light of the global nature of cyber threats and solutions. As noted above, several of the solutions identified by CSRIC III, such as DNSSEC or BGPSEC, will only work if there is ubiquitous adoption. But neither the federal regulatory apparatus nor U.S. communications companies under pressure can demand or achieve that ubiquity. Even if all U.S. players were to implement the identified measures, complete security would still be elusive, because of the global and interdependent nature of our communications system and pathways. While significant amounts of inter-regional Internet traffic flows to or through the United States, significant volumes of traffic and capacity connect directly to hubs outside the U.S. Ineffective or partial solutions are not a sound foundation for mandates or regulation in the U.S.; instead consensus based processes should continue to play out, engaging the global ecosystem.

The FCC should retain its historic role, and disavow any intent to pursue cybersecurity regulation. Rather than expending government and private sector resources developing or threatening to impose standards that are likely to be at least partly irrelevant before they are complete, the Commission should identify more effective opportunities to improve overall cyber security. We look forward to working with the Commission on those opportunities.

2. Reporting or disclosure burdens that aim to provide "assurance" may do more harm than good.

It is unclear what sort of "assurance" the FCC has in mind, but officials have hinted at various disclosure and accountability measures, perhaps through public or regulatory disclosures or certifications. Efforts to seek "assurances" through agency reporting or public disclosures can

---

and rely on consensus standards where possible, standards must be specific and not phrased in a conditional manner because "agencies may confuse regulated parties by incorporating by reference material that is phrased as—and was intended by its drafter to be—nonregulatory."). Recommendations of the sort in CSRIC reports are simply not appropriate bases for regulatory obligations.

be burdensome and do more harm than good. Providing information to regulators and the public is not cost-free. Reporting obligations and informational requests impose burdens on the private sector. Congress recognized such burdens when it passed the Paperwork Reduction Act of 1980, to reduce the paperwork burden that the government imposes on businesses and citizens.[58]

Public disclosure regimes bring their own complications. Economics literature notes that information can affect—but does not necessarily *help*—markets and incentives. "In fact, there are many disadvantages of greater disclosure" in various contexts.[59] Disclosures can shape behavior in undesirable ways. For example, "[i]f there are multiple dimensions of product quality, mandatory disclosure on one dimension may encourage firms to invest in the disclosed dimension but cut back in other dimensions, leading to potential reduction in consumer welfare."[60] But undifferentiated disclosures or characterizations, particularly in an area as nuanced as network, Internet, or mobile security, may not add value or may confuse. Federal Trade Commission research has observed the pitfalls of disclosures in other contexts, concluding that, as a general matter, "[i]ll-conceived disclosures can confuse and even mislead consumers, distort their decisions, and lead to worse choices and outcomes."[61] Ineffective disclosures can "impose unnecessary compliance costs on industry [and] distort seller decisions on product and feature offerings," [62] and can incent private organizations to structure operations to meet static

---

58 Pub. L. No. 96-511, 94 Stat. 2812 (1980), codified at 44 U.S.C. § 3501-3521.

59 I. Goldstein and H. Sapra, *Should Banks' Stress Test Results be Disclosed? An Analysis of the Costs and Benefits*, at 11.

60 D. Dranove and G. Zeh Jin, Quality Disclosure and Certification: Theory and Practice, 48 Journal of Economic Literature 4, 945 (Dec. 2010), *available at* http://www.jstor.org/discover/10.2307/29779704?uid=3739584&uid=2&uid=4&uid=3739256&sid=21104646264737

61 J. Lacko and J. Pappalardo, Federal Trade Commission, *Bureau of Economics Staff Report: Improving Consumer Mortgage Disclosures: An Empirical Assessment of Current and Prototype Disclosure Forms*, at 126-127 (June 2007), *available at* http://www.ftc.gov/reports/improving-consumer-mortgage-disclosures-empirical-assessment-current-prototype-disclosure

62 *Id*. at 128.

reporting requirements, as opposed to focusing their resources on innovating and responding to actual threats. For all these reasons, the government should be reluctant to try and use information to shift market forces in as complex and fast-moving an area as cybersecurity.

3. Incentives are not presently aligned for optimal information-sharing.

Gathering and sharing meaningful information about cybersecurity faces obstacles. Incentives are not properly aligned with respect to sharing information with the government or between private entities. Information provided to the government or advisory committees can be subject to disclosure, for example under the Freedom of Information Act ("FOIA"). Current exemptions may not fully or decisively protect the sort of information the government may want. For example, industry assessments; general capabilities; international standards; and evolving technologies may not fit cleanly within existing exemptions, the contours of which are subject to frequent litigation.[63] Current Administration policy favors broad disclosure under FOIA,[64] but even if the FCC were inclined to shield information, courts—not the agency—often have the last word.[65] Private companies often spend substantial resources to evaluate and protect trade secret, propriety, and sensitive information before it is shared, and then later to try and shield

---

[63] DOJ identifies complexities under Exemption 4, 5 U.S.C. § 552(b)(4), and explains that *c*ourts have had to address several issues, including a narrow approach to trade secrets. *See* Guide to the Freedom of Information Act, Exemption 4, at 264-65, *available at* www.justice.gov/oip/foia_guide09/exemption4.pdf. DOJ notes the counterintuitive teaching that "an agency's promise that information would not be released [is] not considered dispositive." *Id.* at 274. The FCC does not often assert law enforcement and national security exemptions. *See* Federal Communications Commission Freedom of Information Act Reference Guide, at 9 (May 2013), *available at* http://transition.fcc.gov/foia/foiahandbook.pdf. This complexity illustrates the risks of sharing information with the government.

[64] *See, e.g.*, Presidential Memorandum for the Heads of Executive Departments and Agencies Concerning the Freedom of Information Act, 74 Fed. Reg. 4683 (Jan. 21, 2009).

[65] *See, e.g.*, 5 U.S.C. § 552(a)(4)(B) (courts review *de novo* an agency's use of a FOIA exemption to withhold documents, and the burden is on the agency to justify withholding).

information from third-party litigation.[66] It will be difficult for the FCC to provide guarantees that information will not be made public, shared within government, or given to third parties.

Likewise, sharing information *between competitors* poses risks.[67] Recent Department of Justice ("DOJ") and Federal Trade Commission ("FTC") antitrust guidance is helpful, but the private sector still faces compliance and litigation risk.[68] That guidance applies to "a limited category" of "cybersecurity threat information"[69] and may not shield general business information or strategies. Some information is highly propriety and not suitable for sharing outside very controlled circumstances. Thus, risk from sharing information remains salient.[70]

Without clear protections, private companies bear the burden of gathering, analyzing and weighing the risks associated with information sharing and disclosure. Whether it involves the risk of public or third-party disclosure or claims of anti-competitive behavior, uncertainty can be costly, in resources and time, and will remain an impediment. This is why CTIA advocates for the enactment of legislation, like the Cyber Intelligence Sharing and Protection Act ("CISPA") and the Cybersecurity Information Sharing Act ("CISA"), which would alleviate many of the

---

66 *See, e.g.*, *Skybridge Spectrum Found. v. FCC*, 842 F. Supp. 2d 65 (D.D.C. 2012) (denying appeal of FCC decision not to release confidential information in response to FOIA request).

67 *See* Letter from The Coalition Regarding CISPA to The Honorable Mike Rogers and The Honorable C.A. Dutch Ruppersberger (Feb. 12, 2013), *available at* https://www.uschamber.com/letter/coalition-letter-regarding-cispa (information sharing requirements must be accompanied by "an exemption from antitrust laws, which limit exchanges of information") ("Chamber letter").

68 *See* Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information (Apr. 10, 2014), *available at* http://www.justice.gov/atr/public/guidelines/.

69 *Id.* at 7.

70 Indeed, controversies can arise over private standards, in which those dissatisfied with the process or results can litigate. *See, e.g.*, *TruePosition, Inc. v. LM Ericsson Tel. Co.*, No. 2:11-cv-04574 (E.D. Pa. filed July 20, 2011) (claiming that large telecommunications companies "hijacked" standard-setting organizations to set technical standards for future LTE 4G wireless networks to TruePosition's detriment).

current impediments to information-sharing, and improve communications between Internet ecosystem players and the federal government.[71]

Any FCC action that seeks to collect information, provide public assurances and disclosures, or promote the sharing of information, must recognize existing constraints and incentives, carefully consider its goals and objectives, and ensure that any effort does not do more harm than good.

B. The FCC should promote voluntary activity by industry and standards bodies and support existing collaborations.

The Commission should continue to allow existing domestic and international processes to play out on cybersecurity in the communications sector and await direction from Congress on substantive initiatives. CSRIC IV is underway and its work should not be disrupted or diluted. As explained above, many of the issues raised in the PN are being looked at in CSRIC IV. Plus, many of the same organizations interested in this PN are already devoting resources to supporting CSRIC activities. The FCC should continue to let the CSRIC process take the lead.

The FCC could also consider engaging more with international counterparts through the International Bureau and other federal agencies and international bodies, which could help promote better security worldwide. The need for ubiquity throughout the international ecosystem to advance major cybersecurity recommendations demonstrates the need to work with international regulators to improve security worldwide.

Fundamentally, in approaching cybersecurity, the FCC must remain mindful of its long-standing policy of a light regulatory touch, and the limits of its reach into the Internet ecosystem. The FCC has historically left to industry key choices in the technologies, networks, and services

[71] Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013) ("CISPA Bill"); Cybersecurity Information Sharing Act, S. 2588 (2014); *see generally* July 22, 2014 Letter from NCTA, CTIA and USTelecom to The Honorable Harry Reid and The Honorable Mitch McConnell, available at cisa-joint-association-letter-072214.pdf (lauding CISA); *see also* Chamber letter, *supra* n. 67 (urging passage of CISPA).

it provides, giving private entities the "flexibility to deploy the network technologies and services they choose."[72] In promulgating the now-vacated anti-blocking and anti-discrimination broadband rules in its Open Internet proceeding, the Commission chose not to regulate broadband providers' "reasonable network management," which included measures to "ensur[e] network security and integrity."[73] There remain important questions about the limits of the agency's proper reach in this area. The inability to influence vast swaths of the global mobile and internet ecosystems—from application stores to OS developers to global ISPs and end users—confirms that regulatory efforts are likely to be ineffective. The FCC should hew to the "less-is-more" policy that has resulted in incredible benefits to the American economy.

The FCC can help. Information-sharing remains burdened by obstacles which must be addressed by Congress. The communications sector seeks "protections that facilitate the ready and rapid exchange of cybersecurity-related threats, countermeasures and recovery mechanisms in the collective context of the private sector."[74] Protections would rest on three principles:

- Liability protection (with respect to private-to-private and private-to-government sharing);
- Antitrust exemption (with respect to private-to-private sharing); and
- Protection against public disclosure (with respect to private-to-government sharing).

These adjustments are reflected in recent legislative proposals. The FCC should support efforts to reduce barriers to information sharing.[75]

---

[72] *See In re of Implementation of Section 6002(B) of the Omnibus Budget Reconciliation Act of 1993*, 26 FCC Rcd 9664, 9734 (¶ 106) (2011).

[73] *In re of Preserving the Open Internet*, Report and Order, 25 FCC Rcd 17905, 17952, (¶ 82) (2010).

[74] Information Sharing White Paper.

[75] The White House recently voiced its support for such legislation. *See* Michael Daniel, *Strengthening Our Cyber Community*, The White House Blog (Sept. 19, 2014), *available at* http://www.whitehouse.gov/blog/2014/09/19/strengthening-our-cyber-community.

Finally, the FCC can ensure that its actions do not inadvertently change incentives or undermine cooperation. The Public Notice characterizes some entities' earlier support of CSRIC III "recommendations" as a "public[] commit[ment] to implement them."[76] Demanding regulatory "accountability" on pain of prescriptive regulation from entities that voluntarily contribute to evolving best practices may have unintended consequences. A signal from regulators that reporting or transparency obligations might follow voluntary activities may chill collaboration on CSRIC IV activities, and may undermine broader use of the NIST Framework. As the government looks to encourage industry to use and refine existing approaches, it should be wary of creating uncertainty, and should continue to promote the industry-led, voluntary activities that have been so successful for so long.

VI. CONCLUSION

CTIA welcomes the FCC's continued interest in cybersecurity in the communications sector. The threats are real and quickly evolving. Given the nature of these threats, industry's need to rapidly evolve defensive tactics, CTIA encourages the FCC to continue to focus its efforts on continuing to support voluntary industry activity and facilitating collaboration. The FCC should consider how it can use its expertise to support industry, and assist efforts to provide additional incentives to innovate and share information.

[76] Public Notice at 1 and n.3.