Before the Department of Commerce
Washington, D.C.

In the Matter of	**)**	
	)	
Developing a Framework to Improve	**)**	**Docket No. 130208119-3119-01**
Critical Infrastructure Cybersecurity	**)**	

COMMENTS OF CTIA- The Wireless Association

Submitted: April 5th, 2013

CTIA – The Wireless Association
Expanding the Wireless Frontier
1400 16th Street NW, Suite 600
Washington DC, 20036
202-736-0081
www.ctia.org

Michael F. Altschul
Senior Vice President, General Counsel

John A. Marinho
Vice President, Technology and Cybersecurity

TABLE OF CONTENTS

Page

COMMENTS OF CTIA- The Wireless Association

I. INTRODUCTION AND SUMMARY OF COMMENTS

CTIA-The Wireless Association represents all contributors to the global wireless ecosystem, from manufacturers and carriers to software and application developers. Through collaboration and innovation, these contributors have led a mobile revolution that has transformed the global economy.

CTIA has worked for years with its members and policy makers on security and technology issues. The challenges are real and serious. Rapid and crippling threats come from criminals, terrorists, and nation states seeking to damage American industry and the global economy. The private sector has been responding to increasingly aggressive attacks that often appear to be acts of war. For several years, policy-makers have debated how to help the private sector. Some want to expand the tools and protections available to the private sector, while others seek to place increasing responsibility and obligations on the private sector, with or without additional protections.

In February 2013, after several pieces of legislation failed to bridge key policy divides, the President issued Executive Order 13636 and Presidential Policy Directive, PPD-21, directing Executive Branch entities to begin taking action on cybersecurity.[1] Of the several steps outlined in those documents, Section 7 of the Executive Order directs the National Institute of Standards and Technology ("NIST") to "lead the development of a framework to reduce cyber risks to critical infrastructure."

NIST's overall mission is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."[2] CTIA supports the goal of improving the private sector's ability to prevent and respond to cyber threats. NIST's expertise and perspective as a non-regulatory agency can help identify what works, so that entities can better share information and improve on what is already working well.

NIST has been tasked with developing a Cybersecurity Framework made up of "standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[3] The Framework must "incorporate voluntary consensus standards and industry best practices to the fullest extent possible" and be "consistent with voluntary international standards when such international standards will advance the objectives of this order."[4] NIST issued a Request for Information ("RFI") to help it create a "preliminary Framework" that will inform the final Cybersecurity Framework.[5] The RFI

---

1 Executive Order – Improving Critical Infrastructure Cybersecurity, rel. Feb. 12, 2013 ("Executive Order"); Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience, rel. Feb. 12, 2013 ("PPD 21").

2 NIST, General Information, available at http://www.nist.gov/public_affairs/general_information.cfm

3 Executive Order, at § 7.

4 *Id.*

5 National Institute of Standards and Technology, *Developing a Framework to Improve Critical Infrastructure Cybersecurity*, Notice and Request for Information, 78 Fed. Reg. 13024 (Feb. 26, 2013) ("*NIST RFI*"); Executive Order § 7(e).

describes NIST's task in broad terms, posing more than thirty questions across three main areas: *current risk management practices, use of frameworks, standards, guidelines and best practices,* and *specific industry practices*.

Given the complex technical dynamics in cybersecurity, any framework NIST identifies should be performance-based, industry-led, and internationally harmonized. As explained in Part II, the wireless industry is complex, dynamic and global. It benefits from a light regulatory approach, which facilitates flexibility and innovation. This innovation has transformed numerous sectors of the global economy, and if allowed to continue free from regulation and interference, will continue to do so.

As explained in Part III, the industry is making great strides in cybersecurity through voluntary best practices, standards, and user education, which leave diverse participants free to scale responses to their threat environments, security imperatives, and cost-benefit needs. These best practices and standards provide NIST some examples of current procedures and policies that support performance-based, voluntary and flexible approaches.. Industry also relies on consumer and user education. Cybersecurity is challenging precisely because the wireless industry is diverse and open, and consumers demand to control their technology.

With these dynamics as a backdrop, CTIA identifies in Part IV several principles that should inform any Framework relevant to the wireless sector. First, for any approach to be sufficiently flexible, it must be led by industry and avoid technical or operational mandates. Industry participants can identify workable performance-based goals and scalable implementation. Goals for the wireless industry will evolve and can take many forms: continuity of service, transmission integrity, or benchmarks for identity verification and access controls. Government can help industry formulate goals, but should not direct particular goals or methods of achieving them.

In addition to industry-led performance-based goals, international harmonization is key, particularly for wireless. The borderless nature of the wireless ecosystem makes it uniquely transformative but also an attractive target for those seeking to do harm. The United States has an important role to play in fostering cybersecurity, but it needs to work within the global market to foster continued innovation consistent with longstanding U.S policy and values.

CTIA applauds NIST's energy in addressing the diverse issues in the RFI. NIST has a lot to offer industry and policy makers. However, NIST's effort may be constrained because companies may be reticent to publicly share security information, and because policy-makers' goals are not yet clear. NIST can look to existing industry initiatives as it considers how to foster innovation. The Cybersecurity Framework should not be seen as a roadmap for regulation. Rather, industry must be freed to share information and develop techniques that satisfy privately-developed performance goals for cost-effective security across organizations of varied size and sophistication. Regulation should only be considered if those efforts are tried and fail.

II. THE GLOBAL WIRELESS ECOSYSTEM IS DRIVING INNOVATION

A. Mobility is transforming the global economy with flexibility and security.

CTIA agrees with NIST that the United States economy "has become increasingly dependent on information technology."[6] Wireless innovation contributes approximately $150 billion annually to the United States GDP and supports 3.8 million direct and indirect jobs nationwide.[7]

Domestically, U.S. mobile traffic grew 1,275 percent between 2009 and 2012,[8] and the FCC's most recent Wireless Competition Report confirms that data is a key driver. "It is estimated that U.S. mobile data traffic increased 270 percent from 2010 to 2011 and it and that it has more than doubled each year for the past four years."[9] This mobility is affecting key economic sectors. In the energy sector, the penetration of smart meters, an important component of smart grid technology, approached 25% of U.S. electricity consumers in 2011.[10] Likewise, the health care system benefits from mobility. One study expects that by 2016, the U.S. market for remote and wireless patient monitoring systems to track vital signs will reach $20.9 billion, an increase of 436% from 2007.[11] Meanwhile, Near Field Communication (NFC) technology is expected to be utilized by 25% of U.S. mobile phone users to pay for goods in-store.[12] In addition, according to a recent Mobile Work Exchange study, federal employees have increased productivity by an average of nine hours per week using mobile devices, a gain for government of $28 billion, and more than half of workers utilize BYOD.[13]

The exponential increase in the amount of data communicated each day by mobile devices would not be possible without the security enabled by mobile devices and the systems with which they communicate. All elements of the complex wireless ecosystem play a part.

A complex and interrelated "system of systems" comprises the global mobile environment. First, the input, or upstream, segment provides the backbone of wireless communications networks and includes towers, network equipment, backhaul facilities, and spectrum.[14] Second, wireless carriers transmit voice, messaging, and data services over the network.[15] Finally, in the edge, or downstream segment, sophisticated mobile devices

---

6 *NIST RFI*, 78 Fed. Reg. at 13025.

7 *See FCC Chairman Julius Genachowski, Prepared Remarks to International CTIA Wireless 2012*, at 2-3 (May 8, 2012), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-313945A1.pdf ("Genachowski CTIA Remarks"); CTIA – The Wireless Association®, *Today's Mobile Cybersecurity: Protected, Secured & Unified*, at 3 (rel. Oct. 10, 2012) ("CTIA First White Paper").

8 Jimm Phillips, *Increased Spectrum Availability Will Relieve Pressures Created by Rising Data Usage, FCC Wireless Bureau Chief Says*, Communications Daily, Feb. 20, 2013, at 2 (discussing comments by FCC Wireless Bureau Chief, Ruth Milkman).

9 FCC, Sixteenth Annual Wireless Competition Report (¶ 2) (rel. March 22, 2013).

10 GSMA & A.T. Kearney, *The Mobile Economy 2013*, at 33, *available at* http://www.gsmamobileeconomy.com/ ("GSMA Mobile Economy").

11 Nicole Lewis, *Remote Patient Monitoring to Double by 2016*, InformationWeek.com (July 25, 2012), *available at* http://www.informationweek.com/healthcare/mobile-wireless/remote-patient-monitoring-market-to-doub/240004291.

12 GSMA Mobile Economy, at 38.

13 Mobile Work Exchange, *The 2013 Digital Dilemma Report: Mobility, Security, Productivity – Can We Have It All?*, at 3 (Jan. 15, 2013), *available after free registration at* https://www.mobileworkexchange.com/our-research/research-register/2110.

14 *See Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993*, Fifteenth Report, 26 FCC Rcd 9664 (2011) ("*Fifteenth Report*").

15 *Id.*

containing operating systems, applications, content, and mobile commerce connect consumers to the network.[16]

These diverse contributors -- large and small, domestically and worldwide -- share responsibility for cybersecurity and provide multilayered protection. In the input segment, network-based security provides consumers the power to protect their information through device management capabilities, firewalls, secure storage and virtual solutions. Innovative encryption techniques protect email and data in the mobile wireless services segment. And in the downstream segment, effective solutions focus on end-user education and device solutions such as strong authentication and secure connectivity.

B. Domestic and international standard-setting reflect the complexities of this ecosystem.

National and global standards-setting groups play a vital role in the global mobile ecosystem, resolving technical differences, setting standards, and fostering efficiencies. These groups include the Alliance for Telecommunications Industry Solutions (ATIS), the Institute of Electrical and Electronics Engineers (IEEE), the Telecommunications Industry Association (TIA), and the American National Standards Institute (ANSI), as well as the Third Generation Partnership Projects (3GPP and 3GPP2), consensus-driven international partnership of telecommunications standards bodies. For example, the emerging global standard for wireless broadband technology, Long Term Evolution (LTE), was developed by the 3GPP, and IEEE and 3GPP presently are working to develop standards for refinements of LTE and other standards.

NIST states that it "will incorporate voluntary consensus standards and industry best practices to the fullest extent possible" as part of the Framework, which "will be consistent with voluntary international consensus based standards . . . ."[17] This is critical, because these processes reflect the complexities of a global, innovative market, and puts a premium on implementation flexibility, backward-compatibility, and interoperability while avoiding technological obsolescence. Again, working with and through industry-led, global standards-setting bodies greatly minimizes the risk that the Framework will isolate the United States' methods for cybersecurity responses should international bodies like 3GPP take a different path. Moreover, as 3GPP stresses, "[t]he major focus for all 3GPP Releases is to make the system backwards and forwards compatible wherever possible, to ensure that the operation of user equipment is uninterrupted."[18]

NIST seeks "current adoption rates and related information for particular standards, guidelines, best practices, and frameworks . . . ."[19] For products and services, and depending on what a particular standard addresses, it may take approximately 18 months for a new standard to work through international bodies and another 18 to 24 months to be incorporated into products, including application interoperability testing. Some standards, such as the development of application programming interfaces (APIs) might involve a shorter cycle for international

---

16 *Id.*

17 *NIST RFI*, 78 Fed. Reg. at 13025.

18 3GPP, *About 3GPP*, *available at* http://www.3gpp.org/About-3GPP.

19 *NIST RFI*, 78 Fed. Reg. at 13026.

standard setting and product incorporation. A similar timetable applies to network-side standards, such as the TS 33.102 Security Architecture standards developed by 3GPP.

III. THE WIRELESS INDUSTRY IS ADDRESSING CYBERSECURITY THROUGH BEST PRACTICES, STANDARDS, AND CONSUMER EDUCATION.

The RFI seeks information on "the current usage of existing cybersecurity frameworks, standards, and guidelines" and "the applicability of existing publications to address cybersecurity needs . . . ."[20] NIST also seeks more specific industry practices, such as an "organization's policies and procedures governing risk generally and cybersecurity risk specifically" and the "standards, guidelines, best practices, and tools" which "organizations us[e] to understand, measure, and manage risk at the management, operational, and technical levels."[21] These queries are related, so CTIA will address them together and generally, as individual companies may provide appropriate specific responses.

A. The mobile industry responds to evolving threats through industry groups, government partnerships, and standards bodies.

NIST states that the Framework must incorporate domestic and global standards and best practices and provide a "flexible" and "performance-based" approach.[22] With effective cybersecurity measures as the bedrock of continued wireless growth across all sectors of the U.S. and global economy, CTIA's members are actively investing in new solutions to combat cyber threats. CTIA created the Cybersecurity Working Group ("CSWG") to address cybersecurity practices and collaborate with government and industry. Comprised of senior technical and policy representatives from leading companies, CSWG facilitates innovation and cooperation on advanced countermeasures to evolving threats. In addition to working on security issues within the mobile ecosystem, the CSWG has produced white papers for policy makers and has commented on proposals before government and non-governmental bodies.

The mobile industry seeks flexible solutions in collaboration with domestic and global standard-setting groups. These groups have produced myriad standards covering the wireless ecosystem. To the extent NIST "find[s] potential gaps,"[23] any response must fit within the appropriate global standard-setting frameworks and support the voluntary and performance-based solutions which have been -- and will continue to be -- produced.

The mobile industry's blueprint stresses the importance of flexibility. From device manufacturers to network providers to OS developers, the blueprint contemplates unified efforts and independent investment to advance effective cybersecurity solutions. Though cyber threats may be common across industry players at a given moment, entities throughout the mobile space must enjoy freedom to devise their own solutions to evolving threats based on industry-wide best

---

20 *NIST RFI*, 78 Fed. Reg. at 13027-28.
21 *NIST RFI*, 78 Fed. Reg. at 13027.
22 *NIST RFI*, 78 Fed. Reg. at 13025.
23 *NIST RFI*, 78 Fed. Reg. at 13025.

practices, collaborative efforts, and codes of conduct. By contrast, static, standardized security measures will provide a roadmap for hackers and cyber criminals to help focus their attacks.[24]

CTIA supports NIST's efforts to survey current and planned cybersecurity solutions, and encourages NIST to fully examine standards and best practices developed by standards-setting groups. The importance of adaptable industry solutions and international harmonization is evident in Executive Order 13636, which directs the Cybersecurity Framework to "incorporate voluntary consensus standards and industry best practices *to the fullest extent possible*" and "*be consistent with voluntary international standards* when such international standards will advance the objectives of this order."[25] International standard-setting groups such as IEEE, ATIS, and 3GPP resolve technical differences, foster efficiencies, and ensure interoperability and harmonization, and the industry's cutting-edge responses to cyber threats are made possible through coordination with these global and national standards-setting groups and processes.

CTIA and its members also collaborate with federal and local agencies to address cybersecurity. For example, CTIA and its operator members work closely with the National Communications System ("NCS") and the United States Computer Emergency Readiness Team ("US-CERT") to share information and to fortify networks to minimize vulnerabilities. NIST is aware that companies engage in ongoing research and dialogue with it and other agencies like NTIA, Defense Information Systems Agency, and the Department of Homeland Security, in addition to a variety of working groups. Robust public-private partnerships assist the federal government on national security and emergency preparedness. Any initiatives must be coordinated with appropriate public-private efforts to efficiently use resources.[26]

B. A variety of best practices and voluntary standards address cybersecurity.

CTIA agrees with NIST that "there are core cybersecurity practices that can be identified" and which should "be a focus of the Framework development process."[27] Effective cybersecurity is addressed through multi-layered protection throughout the mobile ecosystem, which includes end users. CTIA identifies these best practices and standards as examples of some of the policies and procedures available to manufacturers, operators, and users across the wireless industry. These sorts of tools can be used and adapted, as appropriate, based on an individual, organization, or network's structure, needs, and risk environment. They illustrate the diverse and scalable options available to the wireless ecosystem, which may inform NIST's approach to a cybersecurity Framework.

---

[24] CTIA – The Wireless Association®, *Today's Mobile Cybersecurity: Blueprint for the Future*, at 24 (rel. Feb. 12, 2013) ("CTIA Second White Paper").

[25] Executive Order, at § 7(a) (emphasis added).

[26] These comments do not attempt to catalog the many avenues for collaboration, but examples include the National Security Telecommunications Advisory Committee, which facilitates the provision of advice to the President, and the National Coordinating Center for Telecommunications and the Communications Information Sharing and Analysis Center, which provide operational support. The Communications Sector Coordinating Council helps coordinate national infrastructure protection and response plans. And the National Cybersecurity and Communications Integration Center facilitates communications sector coordination with the cyber protection efforts of the US-CERT.

[27] *NIST RFI*, 78 Fed. Reg. at 13026.

1. Industry has best practices for mobile security, including from CTIA, CSRIC, and MAAWG.

Wireless industry participants look to many best practices for guidance. Particularly relevant best practices have been identified by CTIA, the Communications Security, Reliability, and Interoperability Council (CSRIC), and Messaging Anti-Abuse Working Group (MAAWG). These are examples of best practices. The private sector voluntarily draws upon and follows best practices like these when doing so is appropriate in light of their mission and risk-benefit calculation.

CTIA recently released two White Papers, and is developing a third, identifying available security innovations throughout the mobile ecosystem and describing the blueprint for industry to develop solutions as part of a flexible framework.[28] The Second White Paper illustrates the wide range of mobile threats and lays out the industry's blueprint for collaboration and innovation. The First White Paper outlines a variety of security solutions deployed throughout the mobile ecosystem. For example, encryption methods can protect data residing on a mobile device, such as FIPS 140-2 published by NIST.[29] Available virtual private network (VPN) technology typically requires authentication and uses encryption techniques to safely connect computers and mobile devices to isolated remote computer networks that would otherwise be inaccessible.[30] Existing and evolving two-factor authentication methods utilize digital identifiers or time-based random numbers in addition to passwords to prevent hackers from effectively using stolen passwords.[31] These options for preventive measures are complemented by reactive measures. For example, wireless companies maintain a nationwide database to prevent lost or stolen smartphones from being activated for network use.[32] Similarly, remote wiping can allow end-users to erase data from devices presumed lost or stolen or enterprises to selectively wipe sensitive, work-related data.[33] Anti-virus and anti-malware software is available to protect, detect, and remove malware that can flow between devices and networks.[34]

In addition, the CSRIC addresses cybersecurity best practices, including recommending optimal communications systems security and reliability solutions to the FCC. CSRIC Working Group 2A (WG2A), comprised of security experts from both the private and public sector, focused on telecommunications industry cybersecurity and issued its Best Practices Final Report in March 2011.[35] The Final Report, which aimed to update best practices issued by the Network Reliability and Interoperability Council (NRIC) in 2004, keyed on five vertical areas – wireless, IP services, network, people, and legacy services – and four horizontal areas – identity management, encryption, vulnerability, management, and incident response.[36] Demonstrating

---

[28] CTIA First White Paper; CTIA Second White Paper. CTIA incorporates both the First and Second CTIA White Papers into these comments and attaches them as Exhibits A and B.

[29] CTIA First White Paper, at 20.

[30] *Id.*, at 21.

[31] *Id.*, at 22.

[32] *Id.*, at 18.

[33] *Id.*, at 19.

[34] *Id.*

[35] CSRIC Working Group 2A, *Cyber Security Best Practices, Final Report* (Mar. 2011), *available at* http://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf ("CSRIC WG2A Report").

[36] *Id.* at 7.

that "[r]apid changes in technology continue to evolve in the [w]ireless space," CSRIC WG2A issued 47 new Best Practices for the wireless industry, leaving just five NRIC best practices modified or unchanged.[37] For instance, the Report suggested that "[s]ervice [p]roviders and [n]etwork [o]perators should perform a remote wipe (i.e. reset the device back to factory defaults) when an employee mobile device is lost, stolen, sold, or sent to a third party for repair. Organizations need to have a procedure set for users who have lost their devices."[38] The Final Report also put forth the following general approach to appropriate cyber-threat incident response: preparation, identification, containment, eradication, recovery, and lessons learned.

The MAAWG is an international organization which develops best practices and methods for the mobile messaging industry to bolster online safety. In October 2012, MAAWG issued its Best Practices to Address Online and Mobile Threats, which issued recommendations on how to address new and increasingly sophisticated online and mobile hazards.[39] MAAWG's industry best practices focus on detection and notification, education and awareness, minimizing risk for legal challenges and regulatory oversight, and facilitating industry and government-led collaboration.[40]

2. Several voluntary standards, from ATIS, TIA, 3GPP, 3GPP2 and ISO, guide the wireless industry.

Industry looks to a variety of voluntary standards for guidance on security. While there is a wealth of available industry security standards, the Alliance for Telecommunications Industry Solutions (ATIS), 3rd Generation Partnership Project (3GPP), the Telecommunications Industry Association (TIA), 3rd Generation Partnership Project 2 (3GPP2) and the International Organization for Standardization (ISO) provide good models of such voluntary standards. Private sector entities consider and draw from relevant standards like these, when doing so is appropriate in light of their mission and risk-benefit calculation.

For example, member companies of ATIS define and develop standards and solutions. Accredited by the American National Standards Institute (ANSI), ATIS is also the North American Organization Partner for the 3rd Generation Partnership Project (3GPP). The ATIS Technology and Operations (TOPS) Council Cyber Security Focus Group (CyberSec-FG), comprised of representatives from industry-leading companies, has analyzed the entire wireless ecosystem, from the core to the edge, as part of a phased, end-to-end approach. The CyberSec-FG determined that mapping end-to-end network topology and security zones onto ATIS' Reference Architecture would provide a foundation for developing secure network hardware, trust and identity architectures, and mobile device management. In addition, ATIS has produced hundreds of voluntary NRIC Best Practices.

The 3GPP unites ATIS and five other international standard-setting organizations in an effort to develop international telecommunications industry standards. The 3GPP Systems

---

37 *Id.* at 12.

38 *Id.* at 75.

39 MAAWG, *Best Practices to Address Online and Mobile Threats* (Oct. 15, 2012), *available at* http://www.maawg.org/sites/maawg/files/news/M3AAWG_LAP_Best_Practices_to_Address_Online_and_Mobile_Threats_0.pdf ("MAAWG Best Practices").

40 MAAWG Best Practices, at 14-17.

Aspects (SA) Working Group 3 has responsibility for security in 3GPP systems, including determining security requirements and specifying security architectures and protocols. The Working Group also ensures availability of cryptographic algorithms necessary as part of the specifications. For example, 3GPP TS 35.205 and TS 35.206 provide specifications for the MILENAGE Algorithm set used for 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*. In addition, 3GPP has defined the security architecture, comprised of security features and mechanisms, for mobile networks.[41] Security features are service capabilities that must meet one or several security requirements, and security mechanisms are elements used to accomplish the feature. For example, to achieve the feature of user identity confidentiality by preventing the user's permanent user identity from being eavesdropped on the radio access link, 3GPP developed a mechanism to allow user identification on the radio path by means of a temporary identity on the visited serving network.[42]

A similar relationship exists between TIA, which is also accredited by ANSI, and the 3GPP2 in developing security standards for the cdma2000® cellular technology. TIA Engineering Committee TR-45 drafts and maintains mobile systems standards, including for cybersecurity.[43] Whenever possible, 3GPP2 leverages the standards developed by 3GPP, helping to ensure a uniform level of security across all third-generation wireless systems.

In addition, the International Organization for Standardization (ISO) develops and publishes international standards for risk management. The Information Technology Sector worked with ISO to issue ISO/IEC 27005:2011, which provides guidelines for information security risk management applicable to commercial enterprises, government agencies, and non-profit organizations. ISO standards are particularly helpful because they offer methodological approaches to assessing and managing risk, rather than prescriptive responses or technical solutions. The ISO "has adopted over 13,000 standards that harmonize product specifications"[44] and "play[s] an increasingly important role in encouraging corporations . . . on their own initiative and not in direct response to governmentally mandated requirements."[45]

These best practices and standards are flexible and often performance-based, so they afford industry participants the ability to identify policies and procedures, and customize particular approaches to meet their individualized goals. NIST should consider whether existing models could become inputs to appropriate performance-based goals that leave industry participants free to decide on appropriate implementation and how to achieve meaningful compliance.

C. Security also depends on continued user education.

---

41 *See* 3GPP, *Digital Cellular Telecommunications System (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Security Architecture*, 3GPP TS 33.102 version 11.5.0 Release 11 (Feb. 2013), *available at* http://www.3gpp.org/ftp/Specs/html-info/33102.htm.

42 *Id.* at §§ 5.1.1., 6.1.

43 TIA, *TR-45, Mobile and Personal Communications Systems Standards*, *available at* http://www.tiaonline.org/all-standards/committees/tr-45.

44 Richard B. Stewart, *Part I Courts, Institutions, and Access to Justice*, 1 Jindal Global L. Rev. 41, 45 (2009)

45 David A. Wirth, *The International Organization for Standardization*, 36 B.C. Envtl. Aff. L. Rev. 79 (2008).

The RFI is noticeably silent on user education, a cornerstone of any viable cybersecurity framework. Consumers and businesses own their systems and devices, and they play as vital a security role as any component in the mobile ecosystem. Indeed, end user choices can–often inadvertently—compromise the security of devices and networks, facilitating threats like botnets and distributed denial of service attacks. This is why many of the best practices and standards discussed above emphasize the role of the end user. For instance, CSRIC WG2A updated NRIC Best Practice 7-6-8096 to state that "[s]ervice providers and [n]etwork [o]perators should educate service customers on the importance of, and the methods for, installing and using a suite of protective measures (e.g., strong passwords, anti-virus software, firewalls, IDS, encryption) and update as available."[46] CTIA's First White Paper recommends consumers to check permissions, exercise caution downloading apps, and utilize secure device configurations, among other mitigation techniques.[47] MAAWG's Best Practices for consumers focus on prevention, detection, and remediation, including filtering potentially dangerous email and avoiding unfamiliar Wi-Fi hotspots.[48]

Education is important because users demand control, customization, and privacy. The RFI solicits input on privacy policies and the impact of privacy on risk management and security, specifically asking, "How should any risks to privacy . . . be managed?"[49] The perceived dichotomy between privacy and security is false. Without security, there can be no privacy.[50] Privacy covers what information is protected, and cybersecurity represents how that protection is delivered in the mobile ecosystem.

The wireless industry takes user privacy seriously. In comments to the FCC, CTIA stressed that "[c]onsumers need consistent privacy protections across the board, without regard to the type of technology or company that collects or uses the data."[51] The mobile industry has developed and voluntarily adhered to guidelines based on Fair Information Privacy Principles ("FIPPs"). These voluntary industry guidelines include the "Consumer Code for Wireless Service," a voluntary commitment to provide understandable policies stating how the carrier will use Customer Proprietary Network Information, CTIA's Best Practices and Guidelines for Location Based Services, and efforts by associations such as the Mobile Marketing Association's Mobile Privacy Guidelines. These and other industry privacy policies emphasize the importance of educating consumers and facilitating their control of information.

No one entity can control mobile security. Effective cybersecurity allows industry players to implement flexible standards, best practices, and guidelines informed by performance-based goals. In this regard, end user education is critical. CTIA and the industry are leading in consumer education, continuously working to strengthen what often is the most vulnerable component of the cyber-threat landscape. Industry members are significant contributors to consumer campaigns such as the CTIA's Cybersafety campaign and corresponding portals, the

---

46 CSRIC WG2A Report, at 91.

47 CTIA First White Paper, at 11.

48 MAAWG Best Practices, at 11-13.

49 *NIST RFI*, 78 Fed. Reg. 13028.

50 *See* CTIA Second White Paper, at 4 ("Digital privacy **cannot** exist without cybersecurity.").

51 Comments of CTIA, *Comment Sought on Privacy and Security of Information Stored on Mobile Communications Devices*, FCC Docket No. 96-115, at 5 (July 13, 2012).

FCC's Smartphone Security Checker,[52] the National Cybersecurity Alliance's StaySafeOnline.org portals, ConnectSafely.org, and the National Center for Missing and Exploited Children's NetSmartz.org. In addition, the FCC released its "Ten Cybersecurity Tips for Small Businesses," which include strong passwords and authentication and training employees in security principles.[53]

The importance of consumer education cannot be overstated. Any cybersecurity framework put forth by NIST must address end user education risks and responses.

IV. THE FEDERAL GOVERNMENT MUST PROCEED WITH CAUTION

A. Industry should continue to lead the development of market-driven, flexible solutions.

Any approach to cybersecurity should rely on the market, which already provides strong incentives to maintain and improve security. Empowering industry makes sense because they have flexibility to be nimble in responding to evolving threats.

Particularly in the mobile space, the United States and the rest of the world rely on the marketplace, not heavy-handed regulation, to pick winners and losers. The FCC has been a standard-bearer on this, repeatedly advocating the importance of mobile industry choice with respect to technologies, networks, and services.[54] The FCC's light touch reflects Congress's desire for a market-driven wireless ecosystem.[55] And, Congress has directed a hands-off approach to the Internet, declaring it "the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet . . . unfettered by Federal or State regulation."[56]

These principles are important because the wireless industry supports innovation in countless other, interrelated industries. Congress' policy has been a resounding success, enabling dramatic advances throughout the United States and global economy. FCC Chairman Genachowski emphasized that "the U.S. mobile innovation economy is now the envy of the world" and that "[t]he ecosystem … is innovating in mutually reinforcing ways, a virtuous cycle, creating tremendous value and inventing the future."[57]

---

[52] FCC Smartphone Security Checker, *available at* http://www.fcc.gov/smartphone-security.

[53] Federal Communications Commission, Cybersecurity for Small Business, *available at* http://www.fcc.gov/cyberforsmallbiz.

[54] *See, e.g.*, Federal Communications Commission, *Connecting America: The National Broadband Plan*, at 60 (2010) (stating that the principles of The National Broadband Plan "include support for regulatory frameworks that are pro-competitive, transparent and technology-neutral."). The FCC affords wireless providers "flexibility to deploy the network technologies and services they choose," *In the Matter of Implementation of Section 6002(B) of the Omnibus Budget Reconciliation Act of 1993 Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless*, 26 FCC Rcd 9664, 9734 (¶106) (2011).

[55] *See, e.g., Implementation of Sections 3(n) and 332 of the Communications Act*, 9 FCC Rcd 7988, 8004 (¶ 29) (1994) (explaining that the "overarching congressional goal" was to "promot[e] opportunities for economic forces – not regulation – to shape the development" in the wireless market).

[56] 47 U.S.C. § 230(b).

[57] Genachowski CTIA Remarks, at 3-4.

Relying on the market makes sense because in the area of technical innovation, the government is unlikely to be able to identify, evaluate or predict optimal solutions for diverse industries. Even if the government could keep up with the pace of innovation, there are additional reasons why government should stay out of the way. Technical mandates and regulatory obligations can reduce flexibility and creativity. Economics literature is full of regulatory efforts that "foreclosed innovation, selected 'incorrect' standards, or favored particular incumbent industries."[58] Passive government participation in the market can contribute to technical evolution, but *de jure* standardization can lock in technology too soon relative to market readiness and with too little market participation. Besides being costly, mandates limit the efficiency of private standard setting. Additionally, government requirements are likely to be more difficult to change than voluntary standards.

NIST should be wary of selecting a particular standard or set of approaches. The RFI implies that standardization can achieve economies of scale, but in the area of cybersecurity, standardization presents its own risks. There is utility in maintaining diverse and evolving approaches, because where one standard or approach emerges, bad actors have fewer targets and can focus their energies. As the Technical Advisory Committee to the FCC on mobile issues has noted, "standardization" of mobile device operating systems has benefitted "bad actors" by helping them focus attacks.[59] The same is true of standardization of security solutions: uniformity can provide a roadmap for hackers and cyber criminals.[60] Policy makers should not constrain stakeholders or, despite the best of intentions, set overly-prescriptive standards for rapidly evolving technologies and services.

Encouraging voluntary, industry-led solutions would be consistent with guidelines governing NIST's role setting standards for federal information technology and security. NIST must "evaluate private sector information security policies and practices and commercially available information technologies to assess potential application by agencies to strengthen information security."[61] NIST must "use flexible, performance-based standards and guidelines that, to the greatest extent possible, permit the use of off-the-shelf commercially developed information security products."[62] NIST does not pick winners and losers, but works to "ensure that such standards and guidelines do not require specific technological solutions or products, including any specific hardware or software security solutions."[63] NIST must also "ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks."[64]

---

[58] Michael G. Baumann & John M. Gale, Economic Analysis of the Regulation of MVPD Navigation Devices (2010)

[59] FCC TAC Security & Privacy Work Group, *Longer Term Anti-Malware Recommendations*, at 2 (2012), *available at* http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting121012/TAC-WS&P-anti-malware-recommendations.pdf.

[60] CTIA Second White Paper.

[61] 15 U.S.C. § 278g-3(d)(7).

[62] 15 U.S.C. § 278g-3(c)(7).

[63] 15 U.S.C. § 278g-3(c)(5).

[64] 15 U.S.C. § 278g-3(c)(6).

B. Cybersecurity must be pursued globally, consistent with U.S. values.

The President's Executive Order envisions a Cybersecurity Framework that will "*be consistent with voluntary international standards when such international standards will advance the objectives of this order*."[65] Any approach must be harmonized with ongoing domestic and global standard-setting, while preserving essential U.S. principles of flexibility and industry-led solutions. This is particularly important in mobile, where the universe of contributors, users, and beneficiaries is global.

Consensus-based processes are particularly important in technology and security. "Existing multi-stakeholder processes are better adapted to address Cybersecurity and related issues. Groups such as the Internet Engineering Task Force (IETF) and 3GPP, for example, are actively developing standards and specifications for network and device security – drawing on rapid innovations in engineering technologies."[66] These foundational principles favor flexible standards developed through established standards bodies, like ATIS and 3GPP that work holistically in addressing cybersecurity encompassing different aspects of the mobile ecosystem, e.g. network, applications, devices, etc.

Such coordination must be faithful to core American principles of promoting innovation and flexibility. These values inform the United States' approach to international technology issues. Ambassador Terry Kramer, U.S. Head of Delegation to the World Conference on Internet Communications stated, "our international telecommunications and internet sectors are flourishing . . . precisely because it is an open platform – with open standards-setting, open markets, open networks and the free flow of ideas, content and commerce that is carried over those networks."[67] Using the wireless industry as an example, Ambassador Kramer observed that "the mobile revolution [became] so successful, so fast [through] . . . [i]ndustry-driven standards-setting which brought technological innovation to market at accelerated speeds."[68] NIST should keep these dynamics in mind.

C. The government should not expect NIST's Framework to be importable into federal regulation.

NIST's Framework should not become a platform for increased federal regulation, for which there is not a compelling need. Federal regulators have limited authority and can only act consistent with delegations from Congress. In the mobile space, Congress has made plain that the only regulation properly considered is that for which there is clear-cut need.

In the area of cybersecurity, there is no compelling need for a regulatory response. Indeed, there are serious impediments to regulatory action. The fact that Congress has been debating a regulatory approach underscores the lack of clear agency authority and the absence of any clear policy direction. As a result, NIST's efforts are properly focused on industry choices, and should not be seen as a predicate or blueprint for federal regulatory action.

---

65 Executive Order at § 7(a).

66 Terry Kramer, Remarks to SAMENA (Sept. 9, 2012), *available at* http://www.state.gov/e/eb/rls/rm/2012/197545.htm ("Kramer Remarks")

67 Kramer Remarks.

68 *Id.*

Even if there were authority and NIST evaluation was a proper input to regulatory activity, NIST's process suffers from some practical limitations that render its conclusions a poor foundation for regulation. As mentioned, NIST's goals are somewhat amorphous and broad, so comments are likely to address a variety of different possible outcomes. In addition, NIST is conducting this public inquiry without the benefit of improved incentives and protections for information sharing, so participants may not share some useful information. Given the uncertainties surrounding the possible use of information in regulation, contributors may be more circumspect. These and other limitations threaten to hamper any regulatory efforts that might seek to use the NIST Framework as a platform.

D. Assessing compliance with any Framework will be complicated.

The Executive Order speaks of voluntary participation in cybersecurity programs, and NIST aims for the Framework to be "flexible" and "performance-based." But, the RFI paradoxically states that the Framework "will include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework."[69] Efforts to measure, cajole, or command compliance will be complicated.

First, industries and critical infrastructure sectors are made up of diverse participants, ranging from small businesses to major multinational companies, those with facilities in urban and rural areas, with varied levels of resources and control of inputs. These diverse participants face different risk and threat environments, and divergent cost-benefit calculations in assessing what elements of any standards make sense for them. Devising some set of uniform practices and corresponding "compliance" measures may be challenging.

The absence of governing legislation or guidance on specific goals for the Framework makes it difficult to see how compliance can be demanded, encouraged, or verified. CTIA takes NIST at its word that it "will not prescribe particular technological solutions or specifications," but any compliance regime risks transforming a voluntary, flexible framework into rigid, *de facto* standards, through "incentives," the adoption of regulations, or the transformation of best practices into an enforceable standard of care.

NIST aims "to promote wide adoption of practices to increase cybersecurity,"[70] and also emphasize "compliance," with them. One solution may be to rely on performance-based goals, empower entities to adopt policies and procedures based on an organization's structure, needs and environment, and encourage self-assessment to achieve timely substantial compliance.

E. Obstacles to improved cybersecurity cannot be addressed without legislation.

NIST asks commenters what they see as the greatest challenges in improving cybersecurity across critical infrastructure. Industry participants have long emphasized that they face serious obstacles to more effective responses to cyber threats, and policymakers have debated appropriate solutions for years. These obstacles are real and cannot be addressed without legislation.

---

69 *NIST RFI*, 78 Fed. Reg. at 13025.

70 *Id.*

Cybersecurity is challenging and complex. In order to have the best defense, organizations need to be able to share information—between companies and with government—about potential problems and threats and they need to be able to work together to develop solutions. But private companies are reasonably cautious about sharing information with each other and with the government, both about general practices and individual threats. For example, risk and uncertainty surround sharing malware data that concerns users or others with third parties or the government. Providing information about security processes or vulnerabilities to the government risks public disclosure through Freedom of Information Act requests, and could invite or can be used in oversight functions or enforcement activity. Receipt of information *from* the government also presents challenges, such as in accessing and handling classified information. In addition, the risk of private litigation and civil liability arise after incidents, which can raise significant—and expensive—compliance questions under varied federal and state laws. Finally, companies must consider competitive and antitrust concerns when working together to share best practices or coordinate responses to cyber threats and attacks.

Ironically, these dynamics may hinder NISTs efforts here as NIST seeks industrial policy and security control information through public comments. While the RFI is likely to yield a large volume of information, it may not be comprehensive or adequately specific to help NIST understand current activities and existing gaps.

Confirming the presence of impediments and the need to increase parties' ability to collaborate, Executive Order 13636 directs the Department of Commerce to explore incentives to promote private sector cooperation and increased investment in cyber security.[71] Whatever the result of that examination, legislation will be needed to address obstacles to more effective cybersecurity. Wireless industry participants—like all companies actively engaged in cybersecurity—need to be able to communicate with competitors, federal government agencies, academia and subject matter experts to identify issues and create solutions before there is a problem. Legislation can fix these obstacles, but the government need not regulate or require standards, because industry participants have ample incentive to address cybersecurity. That is why CTIA, like many technology companies and associations, supports the Cyber Information Sharing and Protection Act (H.R. 3523). This legislation was passed in the last Congress and has been reintroduced in the 113th Congress.

V. CONCLUSION

NIST has expertise to bring to bear in helping identify and evaluate current approaches to cybersecurity. The Executive Order's charge to NIST is broad and the RFI is sweeping. Tight timeframes and unresolved policy choices make NIST's job more challenging. In light of these dynamics, CTIA encourages NIST to focus on helping industry identify performance-based goals that maintain a free and global market, and leave room for innovation and flexibility in solutions. CTIA is happy to work with NIST on questions related to the mobile industry, and looks forward to continuing this dialogue.

---

[71] Executive Order 13636, § 8(d) (requiring within 120 days recommendations from the Secretaries of Treasury and Commerce about incentives designed to promote participation in the cyber "program," including whether legislation is requires).

Respectfully Submitted,

CTIA- The Wireless Association

By: /Michael F. Altschul/

/John A. Marinho/

April 5, 2013