Before the Department of Commerce
Washington, D.C.

In the Matter of	**)**	
	)	
Experience With the Framework for	**)**	**Docket No. 140721609-4609-01**
Improving Critical Infrastructure	**)**	
Cybersecurity	**)**	

COMMENTS OF CTIA – The Wireless Association

Submitted: October 10, 2014

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

I. INTRODUCTION AND SUMMARY

CTIA members appreciate the work of National Institute of Standards and Technology ("NIST") on the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework").[1] In response to NIST's request for information on awareness and experience with the Framework,[2] CTIA is pleased to report that there is awareness in the communications sector. Early experiences with the Framework are promising and should be allowed to progress.

The communications sector is fully engaged on cybersecurity and looks forward to working with NIST and in other public-private partnerships on cybersecurity. CTIA members have long focused on protecting the security and privacy of their customers, as well as protecting their networks. The communications sector is hard at work evaluating the Framework, understanding how it can help categorize existing best practices, and determining where industry should focus resources. Because the Framework was just released in early 2014, experiences vary, consistent with the Framework's voluntary, flexible, and scalable approach. The private sector is examining whether and how to leverage the Framework, and how it can be helpful. The Framework is a useful tool for companies considering the right mix of policies and defenses.

The NIST model works because it is non-regulatory, voluntary, and collaborative. The government should continue to look for ways to support the private sector, including efforts to remove barriers and encourage innovation, while avoiding prescriptive regulation or oversight. NIST should continue convening stakeholders, both domestically and internationally. Given the interconnected nature of modern communications and international contributors to innovation and policy, global engagement on cyber will be critical.

II. THE COMMUNICATIONS SECTOR IS AWARE OF THE FRAMEWORK, AND VALUES NIST'S VOLUNTARY COLLABORATIVE APPROACH

NIST asks several questions about awareness of the Framework and its attributes among the private sector, regulators, and internationally. The Framework was released in February 2014. So far, awareness and preliminary uptake are promising. However, the Framework may face headwinds that diminish its utility. To preserve its effectiveness, NIST should manage expectations and emphasize the Framework's voluntary, flexible nature.

A. The communications sector works with NIST and others on cybersecurity.

The communications sector has been engaged with NIST on the Framework and more broadly on cybersecurity. CTIA participated in the Workshops held in 2013, and filed detailed comments.[3] CTIA members found NIST's development process to be collaborative and

---

[1] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf ("Framework").

[2] NIST, Experience with the Framework for Improving Critical Infrastructure Cybersecurity, Request for Information (Aug. 26, 2014), *available at* https://www.federalregister.gov/articles/2014/08/26/2014-20315/experience-with-the-framework-for-improving-critical-infrastructure-cybersecurity ("RFI").

[3] *See* CTIA Comment, NIST, *Request for Comments on the Preliminary Cybersecurity Framework*, Doc. No. 130909789-3789-01 (Dec. 13, 2013), *available at*

effective. The Framework was well-publicized and is being promoted by trade associations including the United States Chamber of Commerce, CTIA, and industry leaders.[4]

The Framework complements ongoing industry work on cyber risk management. For example, the Federal Communications Commission's Communications Security, Reliability, and Interoperability Council ("CSRIC") has a Working Group examining the Framework's application to sub-sectors of the communications industry.[5] CSRIC's work is ongoing, and includes examining challenges unique to smaller and rural elements of the communications ecosystem. The Framework defines a helpful taxonomy for discussing and evaluating risk. It identifies five functions within the security ecosystem: identify, protect, detect, respond, and recover. The Framework also offers guidance about how to assess status and progress against each function. CSRIC will consider all these parts of the Framework.

In addition to work with NIST and CSRIC, the communications industry works with sector-specific groups, non-governmental organizations, and others to continually improve cybersecurity. Several best practices apply to the communications sector, including wireless network operators. They include CSRIC recommendations, International Organization for Standardization ("ISO") standards, International Telecommunication Union ("ITU") documents, Payment Card Industry ("PCI") standards, and standards recommended by the SANS Institute.

The communications sector also works with various public-private partnerships on cyber. For example, the Communications Sector Coordinating Council ("CSCC") enables companies to share information and lessons learned. Many are active in the Communications Information Sharing and Analysis Center ("Comm-ISAC"), the FCC's CSRIC and Technical Advisory Council ("TAC"), the President's National Security Telecommunications Advisory Council ("NSTAC"), and non-profit associations.[6] These efforts complement the Framework's goal of promoting voluntary innovation and information-sharing.

Non-governmental efforts, like the Cyber Threat Alliance ("CTA"), confirm industry's commitment to cybersecurity. In the CTA, cybersecurity practitioners "have chosen to work together in good faith to share threat information for the purpose of improving defenses against advanced cyber adversaries across member organizations and their customers."[7] The goal is "to disperse threat intelligence across all member organizations in order to raise the overall

---

http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html; CTIA Comment, NIST, *Developing a Framework to Improve Critical Infrastructure Cybersecurity*, Doc. No. 130208119-3119-01 (Apr. 5, 2013), *available at* http://csrc.nist.gov/cyberframework/rfi_comments_2013.html.

4 *See* RFI, Awareness Question 8 (inquiring about outreach and education on cyber risk management).

5 *See* 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.

6 *See* CTIA, *Today's Mobile Cybersecurity: Information Sharing*, 21 (Sept. 9, 2014), *available at* http://www.ctia.org/docs/default-source/default-document-library/ctia_informationsharing.pdf ("CTIA Information Sharing White Paper) (*e.g.*, CTIA, the National Cable & Telecommunications Association (NCTA), and U.S. Telecom Association (USTA)).

7 Cyber Threat Alliance Homepage, *available at* http://www.cyberthreatalliance.org/*; see also* Tara Seals, *McAffee, Symantec, Fortinet, and Palo Alto Launch Cyber Threat Alliance*, InfoSecruity Magazine (Sept. 12, 2014), *available at* http://www.infosecurity-magazine.com/news/mcafee-symantec-fortinet-palo-alto/ ("A group of security heavy hitters—McAfee, Symantec, Fortinet and Palo Alto Networks—have come together to … drive a coordinated industry effort against cyber-adversaries through deep collaboration on threat intelligence.").

situational awareness of group members." Such efforts have an international reach, and can be leveraged at NIST to promote international awareness and consensus.

B. There is awareness of the Framework throughout the communications sector and relevant federal agencies.

NIST asks about "awareness of the Framework and its intended uses among organizations."[8] In the communications sector, parties are aware of the Framework and that it is designed to be a voluntary risk management tool that builds on existing standards and practices.

Industry is examining how the Framework maps onto their practices and across sub-sectors. The communications sector is engaged and outreach is being done by our organization and individual companies. Communications companies have found that the Framework is a useful tool as they consider the right mix of approaches. For companies with more sophisticated defenses already in place it may not provide new insights, but it is a helpful tool for others. Because the threat landscape varies across sectors, each sector must balance its cybersecurity needs when considering the Framework. This is certainly true in communications, where subsectors faced different threats, which have varying risk profiles. For example, wireless and wireline ISPs face significantly different threats from botnets: botnets pose a serious threat to PC-users, but have a very low incidence rate on wireless devices.[9]

NIST asks about regulatory agencies' awareness of the Framework.[10] The Department of Homeland Security is intimately involved in Administration activity affecting the communications sector. The FCC is well aware of the Framework, with several agency officials engaged. The FCC participated in the development of the Framework and has asked its federal advisory committee, the CSRIC, to examine existing best practices to ensure they are sufficiently aligned with the Framework. The FCC filed comments as required by the Executive Order on Improving Critical Infrastructure Cybersecurity, but has not made those comments public.[11]

It is important that agencies remain committed to the voluntary approach embodied in NIST's work. The possibility of deviation from this voluntary, collaborative model is one of the main challenges facing the Framework.[12] The FCC is pursuing a "new regulatory paradigm" for cybersecurity that involves industry leadership, and has issued a Public Notice requesting feedback on implementation of earlier voluntary cybersecurity guidelines issued by CSRIC.[13] This "new regulatory paradigm" remains unclear. The FCC appears to be contemplating its role

---

[8] RFI discussion; *see also* RFI Awareness Questions 1-4.

[9] Indeed, the risk of mobile smartphone malware infection is less than two percent in the U.S., which is one of the lowest in the world, and significantly lower than the rates in Germany, Russia, and India. *See* Kaspersky Labs, IT Threat Evolution 1Q 2014, 23 (April 17, 2014) *available at* http://www.securelist.com/en/downloads/vlpdfs/q1-it-threats-en.pdf. *See also* Kaspersky Labs, IT Threat Evolution 2Q 2014, 28 (August 4, 2014) *available at* https://securelist.com/files/2014/08/KL_Q2_IT_Threat_evolution_EN.pdf.

[10] *See* RFI Awareness Question 7.

[11] *See* Executive Order 13636, Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity ("Executive Order").

[12] *See* RFI Awareness Question 5.

[13] The FCC recently changed the mission of current CSRIC WG 4, which was originally tasked with evaluating how the NIST Framework maps onto practices implemented by various communications sub-sectors.

and may take a more assertive posture that contemplates oversight or regulation. Prescriptive regulation, reporting obligations and aggressive regulatory agency oversight are not the best way to address cybersecurity. Requirements to adopt certain practices or periodically report on uptake should be avoided. Such requirements may cause organizations to "meet the standard" and discourage initiatives to address evolving threats. Public or regulatory disclosure or reporting obligations will impose burdens on industry. Any action that could be perceived as having a regulatory overtone threatens to limit the effectiveness of collaborative efforts, like NIST or CSRIC, or fragment the Framework as agencies take it in disparate directions.

NIST asked about international awareness.[14] International awareness appears to be broadening, and there is genuine interest in what the U.S. is doing on cybersecurity. Because of the interconnected nature of modern communications and the global wireless ecosystem, solutions require international collaboration. Some countries appear to awaiting measurable change in industry and government before committing to something like the Framework. The United States should avoid fragmentation of cybersecurity between countries by condoning regulation, lest foreign powers decide to impose conflicting regulatory burdens, or use security as an impediment to trade and openness.

CTIA encourages NIST to continue raising awareness of the Framework and its voluntary nature. This is the best way to improve awareness.[15] Given the fast pace of technological change and the global nature of cybersecurity challenges, policy-makers should continue to focus on collaborative processes. NIST is the ideal convener to work with small to medium businesses, local, tribal, state, and federal agencies, and international bodies, to promote appropriate voluntary use of the Framework and other improvements to cybersecurity.

III. WIRELESS SECTOR EXPERIENCE INCLUDES ADAPTING AND USING THE FRAMEWORK ON A VOLUNTARY BASIS, AS INTENDED.

A. The communications sector is using the Framework to evaluate and complement existing risk management activities.

NIST asks how the Framework is being used.[16] It is still early in the Framework's development and work is underway to make it more useful for the communications sector. The communications sector has long been engaged in cyber risk management; the Framework complements existing effort. An early benefit of the Framework has been its common language, which the sector uses to identify, analyze and map existing practices and standards.[17]

Communications sector companies "understand the importance of managing cyber risk," and have been employing appropriate industry best practices and international standards referenced in the Framework for many years.[18] These companies include cybersecurity risk in their broader risk management evaluation and invest heavily in cybersecurity activities,

---

14 *See* RFI Awareness Question 6.

15 *See* RFI Awareness Question 5 (asking for comment on opportunities to improve awareness), and 9 ("What more can be done to raise awareness?")

16 *See* RFI Experience Questions 1-10.

17 *See* RFI Experience Question 2.

18 *See* RFI Experience Question 1.

processes, and R&D. Many employ solutions that are more robust than those in the Framework. Many carriers have policies and procedures that map to NIST SP-800 series publications, ISO standards, accepted security principles, and other practices developed via policy groups such as the FCC's CSRIC. Sophisticated customers require that service offerings conform with standards specific to their sector. Customers are increasingly aware of cybersecurity risks and see the Framework as a useful tool in determining how to best defend themselves against risks.[19]

NIST inquires about the utility of the major components of the Framework (the Core, Profile, and Implementation Tiers).[20] They are still being assessed and, because they were intended to be flexible and voluntary, may not make sense for each organization. The Core functions seem to be helpful, and are being used to map best practices, as explained. It is still too early to evaluate how helpful each component is, so NIST and agencies should not have firm expectations about how they will be used. Different sectors have different cybersecurity risk profiles. Each sector must have the flexibility to implement necessary solutions relevant to the problems that they actually face. A one-size-fits-all approach is unworkable.

Thus far, the Framework is being used as contemplated.[21] For example, Framework Section 3.4 suggests using it to help "identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs."[22] In the short time that has passed since February 2014, the communications industry has been trying to understand where existing efforts have been focused, in order to identify areas for future attention. CSRIC's Working Group 4 is assessing current practices against the five functions from the Framework and the wireless industry is engaged in independent research to map best practices to the Framework, identify areas for future attention, and develop risk indicators to better assess and project risk. Work is ongoing, and will help assess the best way to utilize the Framework and where to focus future innovation.

The common language of the Framework has been helpful. Section 3.3 provided examples of how the Framework's taxonomy could be used "to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure services."[23] Companies communicate about cybersecurity, and as appropriate given their regulatory and business profiles, may communicate about "the effectiveness of their cybersecurity risk programs." Each organization assesses for itself how to communicate with up and downstream segments as well as the end user.[24]

These uses complement industry work in a variety of public-private partnerships.[25] CSCC was created by DHS as one of 16 sector coordination councils established under the Critical Infrastructure Partnership Advisory Council to ensure communications networks and systems are secure, resilient, and rapidly restored after a disaster. Comm-ISAC enables voluntary collaboration and information sharing on vulnerabilities, threats, intrusions, and

---

19 *See* RFI Experience Question 6.
20 *See* RFI Experience Question 7.
21 *See* RFI Experience Question 8.
22 Framework at 15.
23 *Id.*
24 *See, e.g.*, RFI Experience Question 8(d), (e).
25 *See* CTIA Information Sharing White Paper at 12.

anomalies from multiple sources and to perform analysis to avert or mitigate the impact upon the nation's telecommunications infrastructure. The President's NSTAC includes over 30 members that make recommendations on industry-government cooperation. In addition, the National Cybersecurity and Communications Integration Center ("NCCIC") monitors, tracks, and addresses communications vulnerabilities, intrusions, exploits, and incidents across federal agencies and the private sector. Several nongovernmental organizations address cybersecurity, including the CTA, the Internet Engineering Task Force ("IETF"), and the Alliance for Telecommunications Industry Solutions ("ATIS"). The Framework will help these efforts.[26]

Some in the Administration seek specific metrics to judge the Framework's effectiveness and evaluate cybersecurity risk management.[27] Metrics are not the subject of this RFI, and in any event such a discussion is premature. Work on aligning the Framework may include metrics or success measures. In the communications sector, CSRIC's Working Group 4 has as subgroup looking at metrics and what information would be reasonable, useful, relevant, and obtainable. That is the best way to consider metrics.[28]

NIST asks about use of the privacy methodology in Section 3.5.[29] CTIA appreciates that NIST included a process-based privacy methodology in version 1.0 of the Framework. This tailored, process-based methodology can help large and small organizations in diverse sectors. A more detailed privacy methodology might discourage use of the framework. Companies currently employ process-based controls to address privacy risks in their organizations, consistent with the privacy methodology. Because each organization is unique, CTIA does not believe that further detailed guidance would be useful, and in fact may impair flexibility that companies need to address privacy concerns that arise with fast technological developments.

B. NIST should examine incentives and information-sharing to support voluntary collaboration.

NIST inquires about what activities can be expanded or initiated to promote use of the Framework.[30] NIST should focus on implementing participation incentives, reducing burdens to information-sharing, and reinforcing the idea that the Framework is purely voluntary.

In order to promote the Framework, incentives should be revisited. Incentives such as cybersecurity insurance, grants, process preference, liability limitations, streamlined regulations, public recognition, rate recovery for price regulated industries, and cybersecurity research, are imperative to making buy-in to the voluntary Framework ubiquitous throughout critical

---

[26] *See, e.g.*, RFI Experience Question 8(e).

[27] *See* Charlie Mitchell, *White House Seeks More Industry Input on Cybersecurity "Metrics"*, Inside Cybersecurity (Oct. 1, 2014).

[28] *See* RFI Experience Question 10.

[29] *See* RFI Experience Question 8(c).

[30] *See, e.g.*, RFI Experience Question 9.

infrastructure entities.[31] Incentives are an important piece of the President's vision for improving critical infrastructure cybersecurity and must be part of the solution.[32]

In addition, information sharing can be improved. Existing legal barriers to information-sharing limit what companies share with each other and with the government. Threats of legal action based on disclosures, either through Freedom of Information Act ("FOIA") challenges or from the plaintiff's bar also chill information-sharing. Federal legislation, like the Cyber Intelligence Sharing and Protection Act ("CISPA") in the House and the Cybersecurity Information Sharing Act ("CISA") in the Senate, would improve information-sharing between companies and with the federal government. NIST and other federal entities involved in cybersecurity should do what they can to support such legislation.[33]

Finally, NIST should continue to reinforce the voluntary nature of the Framework. Expectations about voluntary use of the Framework remain prevalent, so there is not yet a concern that NIST has lost ground on this front. To ensure that this expectation continues to be met, regulators should resist the urge to demand immediate results and regulate, which would lead to fragmentation. Since the Framework was released in February 2014, there has not been much time yet to fully evaluate its usefulness and implications. Agencies should support NIST's work, recognizing that the Framework requires time to evaluate and use.

IV. NIST'S ROADMAP IDENTIFIED ISSUES TO BE TAKEN UP IN THE FUTURE

The NIST Roadmap highlights issues that NIST may address in the future.[34] NIST has done a good job identifying areas for future consideration and seems, correctly, to view the Framework and associated efforts as living documents. It is critical that NIST remain a convener of private sector innovation. This will keep the Framework relevant in the future. Given the pace of innovation and other activity ongoing, it would be premature for NIST to address some of the issues identified in the Roadmap. CTIA comments on a few of the issues.

NIST should let the market lead on conformity assessment. NIST intends to work with "[p]rivate sector standards owners, consortia and others who manage conformity assessment programs to help all stakeholders understand how these programs can be further leveraged by those who have the need for conformity demonstration" and with "private and public sector entities that have a need for conformity demonstration, to help understand how these organizations can leverage existing programs."[35]

---

[31] *See* Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, White House blog, (Aug. 6, 2013), *available at* http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

[32] *See* EO, § 8(d) (instructing the Secretary of DHS to coordinate establishment of a set of incentives designed to promote participation in the voluntary critical infrastructure cybersecurity program).

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

[34] *See* NIST Roadmap for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf ("Roadmap").

[35] *Id.* at 5.

Any government attempt to establish assessment, white-listing or other activities would be cause for concern. Areas where conformity assessment might be useful are technically complex and evolving. Government endorsement of best practices threatens to pick winners and losers, and may ossify technical innovation at the level of the conformity assessment. A government-approved "seal of approval" could provide bad actors a guide to common practices, crowd out private initiatives, and encourage other governments to promote their own approaches. In any event, market forces are likely to make government action on conformity assessment unnecessary. In a highly competitive wireless market, participants maintain security and innovate to win and retain customers. Evolving demand for security information and services will drive the market, including for product or service assessments.

NIST should continue to foster international engagement and alignment. NIST plans to communicate the Framework internationally, including to foreign governments, industry stakeholders, and standards groups "to ensure the Cybersecurity Framework remains aligned and compatible with existing and developing standards and practices."[36]

The wireless, Internet, and tech industries have complex global ecosystems. Borders are virtually irrelevant to cyber threats and responses, and many solutions require ubiquitous implementation. NIST should continue to engage the international community. As stated above, the international community seems to be watching to see if the Framework is successful. Encouraging voluntary processes internationally will help U.S. companies maintain flexibility to combat threats, and will avoid duplicative or contrasting regulatory burdens. Activities are underway in the private sector, which could be leveraged on a voluntary basis to expand the global cybersecurity discussion. Avoidance of prescriptive regulation and reporting requirements here is essential to preventing similar burdens overseas.

Attention to supply chain issues must recognize complexities and avoid impeding commerce. NIST's Roadmap identifies supply chain security as a key part of risk management. CTIA members agree, and various activities are underway that address supply chain security. As noted, the Internet and mobile ecosystems are truly global. This is why CTIA members would have concerns about any effort to create U.S.-specific guidelines, set private security standards, or undermine industry security efforts. The U.S. should avoid encouraging efforts to impose barriers to the importation of IT technologies based on country of origin. The government should focus on how IT is designed, built, and maintained versus its geographic point of origin. As the government evaluates IT and technology production and sourcing, the focus should be on commercially practical best practices and global standards that reflect the complexities in this area, including differences in hardware and software sourcing models. In particular, mutually recognized international agreements will be important.

NIST should approach technical privacy standards with care. NIST recently embarked on an initiative to develop objectives and a risk model for privacy engineering, with an eye toward developing controls and metrics as part of a privacy engineering standard. CTIA believes that this new NIST privacy engineering initiative should not address substantive privacy objectives, which properly are the domain of policymakers, but rather should focus on cataloguing, in a policy neutral manner, how privacy engineers accomplish various privacy-by-

[36] Roadmap at 7-8.

design or information management processes they are tasked with developing. In other words, the NIST privacy engineering initiative would pivot away from addressing what *should* be done in the privacy engineering field to identifying what *is* being done in the privacy engineering field. Like the framework and the privacy methodology, this would require input from numerous and varied stakeholders, both within and without the critical infrastructure. With other trade associations, CTIA recently sent a letter to NIST in connection with the privacy engineering initiative that more fully describes its concerns and suggestions for NIST to advance the field of privacy engineering.

V. CONCLUSION

CTIA applauds the inclusive approach that NIST has taken to formulating the Framework, and encourages NIST to continue its work in this same successful manner. Further awareness and uptake of the Framework depend on its voluntary nature. Prescriptive regulations or reporting requirements related to the Framework will stifle its usefulness and create unnecessary burdens. NIST and others in the government should foster true collaboration and information-sharing by supporting venues that are free from regulation. These efforts will lower barriers to information sharing that exist today and improve cybersecurity efforts across the board.