Before the
National Institute of Standards and Technology
DEPARTMENT OF COMMERCE
Washington, D.C. 20230

In the Matter of	)	
	)	
Views on the Framework for Improving	)	Docket No. 151103999–5999–01
Critical Infrastructure Cybersecurity	)	

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association (NCTA)[1] hereby submits its comments in response to the Request for Information[2] issued by the National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce in the above-captioned proceeding.

The Request for Information (RFI) seeks information on the ways in which the "Framework for Improving Critical Infrastructure Cybersecurity" (the "Framework")[3] is being used to improve cybersecurity risk management, the value of different portions of the Framework, and whether it needs to be updated. NIST also seeks comment on long-term governance of the Framework. NCTA is pleased to provide these comments on behalf of our member companies.

---

1 NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 80 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of broadband service after investing over $230 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 28 million customers.

2 Department of Commerce, National Institute of Standards and Technology, *Views on the Framework for Improving Critical Infrastructure Cybersecurity*, Docket No. 151103999–5999–01, 80 Fed. Reg. 76934 (Dec. 11, 2015) ("RFI").

3 *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, National Institute for Standards and Technology, Feb. 12, 2014 ("*Cybersecurity Framework*" or "*Framework*").

I. CABLE OPERATORS CONTINUE TO USE THE CYBERSECURITY FRAMEWORK TO ENHANCE EXISTING CYBERSECURITY PRACTICES

NCTA's member companies are at the cutting edge of developing and implementing practices and techniques for identifying and addressing cybersecurity risks and vulnerabilities. The Framework is a key resource for the cable industry and the overall communications sector. It acts as a comprehensive guide for evaluating cyber readiness and as a compendium of effective cyber defense processes, techniques, and practices. For cable companies, who provide broadband service to most American households, securing and protecting the network is a top business priority. As a result, cable operators treat cybersecurity as a central component of their enterprise risk management strategy and have committed tremendous resources to addressing constantly-changing and pervasive global cyber threats. The Cybersecurity Framework is a key tool for helping operators evaluate and communicate about cybersecurity risks.

As NCTA has previously noted, the cable industry as a whole has taken steps to promote awareness of the Framework and provide information on using its unique risk management approach to cable operators both large and small.[4] NCTA's Cybersecurity Working Group, comprised of cybersecurity and technology personnel from member companies, meets regularly to share information on the latest threats and cyber defense tools. The Framework is useful as a source of shared language and techniques for discussing complex strategies and techniques whose specific implementations often differ dramatically between organizations. The NCTA Working Group encourages member companies to draw upon the Framework's language and techniques when discussing and conducting cyber risk management, and to use it to complement

[4] *See* NCTA Comments filed in Dkt. No. 140721609-4609-01 at 3-8 (Oct. 10, 2014) (describing how cable companies have sought to expand awareness of the framework).

existing business and cybersecurity operations. The informative references to cybersecurity standards, guidelines and practices continue to be relevant and useful.

NCTA member companies also work with the Department of Homeland Security, the Sector Specific Agency for the Communications Sector, through the Communications Sector Coordinating Council (CSCC), which is comprised of representatives from major communications companies and trade organizations, both large and small, across the industry. Cable operators work closely with other CSCC members to improve cybersecurity awareness and coordinate communications sector-wide planning to promote cybersecurity policies and practices in member companies. NCTA member companies play a leadership role in the Communications Information Sharing and Analysis Center ("Comm-ISAC"), which facilitates analysis and voluntary information sharing on threats to communications networks.[5] Cable operators also continue to participate in the DHS's Framework-based initiative, the Critical Infrastructure Cyber Community (C^3) Voluntary Program, which encourages participants to increase awareness of the Framework and adopt cyber risk management as a component of an overall enterprise risk management strategy.

The cable industry has also participated in efforts to review the Cybersecurity Framework in conjunction with the Federal Communications Commission's Communications Security, Reliability, and Interoperability Council (CSRIC). In CSRIC IV, concluded in March 2015, cable industry participants helped encourage adoption of elements of the framework that serve as best practices for the communications sector as a whole. In particular, the CSRIC IV Working

[5] Comcast, Cox Communications, and Time Warner Cable are all members of the National Coordinating Center for Communications (NCC), which is the designated ISAC for telecommunications. *See* US-CERT, Department of Homeland Security, *The National Coordinating Center for Communications (NCC), at* https://www.us-cert.gov/nccic/ncc-watch (last visited Feb. 23, 2016) (listing Comcast, Cox Communications, and Time Warner Cable as industry representatives to the NCC).

Group Four (WG4) Final Report on Cybersecurity Risk Management and Best Practices identified the NIST Framework as a "seminal document in organizing risk management activities across a broad global landscape" and encouraged communications companies to "adapt the NIST Cybersecurity Framework approach to cybersecurity risk management to their own operations and networks."[6] The WG 4 Final Report also noted that use of the Cybersecurity Framework "provides a consistent cybersecurity risk management approach and a common taxonomy to improve internal and external communications regarding cybersecurity risk management."[7]

That common taxonomy and language for cybersecurity risk management is already proving useful as CSRIC V gets underway. CSRIC V Working Group 5 (WG5) is set to discuss Cybersecurity Information Sharing and includes a wide range of industry participants from cable operators and telephone companies to internet security vendors. The Cybersecurity Framework's common language for discussing how to manage cybersecurity risks is a key contribution to discussion and coordination between such diverse organizations.

While cooperation and coordination with government stakeholders in the cybersecurity ecosystem is one component of the cable industry's cybersecurity work, industry-led groups are the key to cooperative development and propagation of network security techniques and best practices. Cable operators participate in a wide array of organizations that engage in cyber-security work, including the Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG), the Internet Engineering Task Force (IETF), and the Alliance for Telecommunications Industry Solutions. These organizations approach cybersecurity using a

---

6 FCC, Communications Security, Reliability, and Interoperability Council IV, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report,* at 9-10, *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

7 *Id.* at 25.

collaborative, multi-stakeholder process that enables the rapid adoption of flexible best practices that are able to be quickly implemented by participating companies despite their diverse array of network technologies and organizational structures.

NCTA member companies contribute frequently to both M[3]AAWG and the IETF. Cable operator representatives played a key role in authoring M[3]AAWG's report on *Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks*[8], now embraced across the communications industry as a common platform for building a network malware management strategy. Through the IETF, cable industry engineers have contributed to the development of DNS authentication technologies (DNSSec) and secure routing protocols (BGPSec). As cable industry engineers work in M[3]AAWG, IETF, and other industry-led groups to develop the next generation of cybersecurity techniques and network best practices, the Framework's risk management taxonomy will help guide discussion and encourage each organization to evaluate cybersecurity risk as an essential component of network management.

II. ONE COMPONENT OF THE FRAMEWORK IS NOT WELL-SUITED TO MODERN CYBERSECURITY BEST PRACTICES

Overall, NCTA member companies have found the Framework's risk management structure's focus on specific cybersecurity outcomes to be very useful. As noted above, the Framework has helped to establish a common vernacular and taxonomy across our members' businesses when discussing cybersecurity and risk management. Out of the Framework's three major elements, the Framework Core has proven to be the most useful part of the Framework. The Framework Core's five concurrent functions – Identify, Protect, Detect, Respond, and Recover – help guide organizations toward a better understanding of cybersecurity risk

[8] *Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks*, Messaging Malware Mobile Anti-Abuse Working Group (July 2009) ("*Best Practices Report*"), *available at* http://www.maawg.org/system/files/news/MAAWG_Bot_Mitigation_BP_2009-07.pdf.

management without being prescriptive or becoming a compliance tool. The informative references to existing standards, guidelines, and practices have proven to be useful to our member companies. When any gaps are identified in existing cybersecurity programs and practices, the informative references provide a good first step towards developing and implementing new practices that suit an organization's unique circumstances.

While NCTA member companies have found the Framework Core a valuable contribution towards communicating cybersecurity risk, the Implementation Tiers have not proven useful. The Tiers do not reflect modern best practices used by our member companies in their technology development programs. The tiers concept in the Framework is based upon the capability maturity model previously used for software and product development. Capability maturity models have proven to be too structured and rigid for areas such as software development and cybersecurity that are constantly evolving. Rather than providing a forward looking way to evaluate cybersecurity risk, the Implementation Tiers look toward checklists, an approach that will be quickly outdated. Software and cybersecurity development today should look toward the Agile programming model for inspiration. The Agile model emphasizes continuous improvement of software and constant evaluation and improvement throughout the development process.[9] Cybersecurity requires a similar, constantly reflective development process. An Agile-inspired development model is a better fit for cybersecurity risk management

[9] *See generally e.g.* Software Engineering Institute, Carnegie Mellon University, *CMMI or Agile: Why Not Embrace Both, at* http://resources.sei.cmu.edu/asset_files/TechnicalNote/2008_004_001_14924.pdf (last visited Feb. 19, 2016) (comparing Agile development methods and CMMI (Capability Maturity Model Integration) best practices); Cisco, *Agile Cyber Security – Security for the Real World, Architectural Approach, at*http://www.cisco.com/web/ME/connect2014/saudiarabia/pdf/osama_al_zoubi_Fahad_aljutaily_agile_cyber_security_security_for_the_real_world_architectural_approach.pdf (last visited Feb. 19, 2016) (describing how Agile development methods can apply to cybersecurity risk management); GovLoop, *–Creating an Adaptive Cybersecurity Strategy and Culture Through Agile Cybersecurity Action Planning (ACAP), at* https://www.govloop.com/community/blog/creating-adaptive-cybersecurity-strategy-culture-agile-cybersecurity-action-planning-acap (last visited Feb. 19, 2016) (describing how Agile development methods can enhance organizational flexibility for cybersecurity threat assessment and response).

programs, reflecting the fluid nature of cyber threats and the corresponding need to quickly respond and adapt defensive measures.

III. NIST SHOULD CONTINUE TO PROMOTE THE FRAMEWORK'S VOLUNTARY, BUSINESS-DRIVEN AND FLEXIBLE NATURE

The Framework stands as a major achievement in aligning government policy, business, and technological approaches to managing cybersecurity risk for systems and processes involved in the delivery of critical infrastructure services. It successfully does this in a voluntary, flexible and business-driven manner. In this context, NIST asks "what steps should be taken to prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014.[10] Congress identified NIST as the ongoing facilitator of the "voluntary, consensus-based, industry-led" Framework and in this role it should continue to promote to federal and state regulatory agencies that the Framework provides guidance for organizations to "manage cybersecurity risk in a cost-effective way based on business needs *without placing additional regulatory requirements on businesses*."[11]

Indeed, it would be counterproductive to the voluntary, business-driven approach to cybersecurity affirmed by Congress and federal agencies for state regulatory agencies to develop mandatory cybersecurity oversight programs that would be inconsistent with federal policy. Moreover, detailed compliance and reporting regimes are ill-suited to a dynamic, highly sophisticated cyber threat landscape, and would hamper innovation and continual refinement of

[10] RFI at 2; the Cybersecurity Enhancement Act of 2014 directs NIST to "on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures and processes to cost-effectively reduce cyber risks to critical infrastructure." Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274 § 101 (a) (as codified in 15 U.S.C. § 272(c)(15)).

[11] Cybersecurity Framework at 1 (emphasis added).

best practices in combatting cyber threats. The Framework is on the right track -- duplicative, conflicting, and burdensome regulatory mandates will impede its continued success. We therefore urge NIST and its federal partners to continue to support public-private partnership models, such as the Communications Sector Coordinating Council (CSCC) and CSRIC, which have worked well in the area of cybersecurity.

Finally, NIST requests comment on whether it should consider transitioning some or all of the Framework's coordination to another organization, such as an international standards organization. First, the cable industry believes that NIST has done an outstanding job shepherding this process and overseeing its implementation. Second, given the dynamic nature of the problem, NCTA does not believe that standards organizations are best suited to developing the type of framework called for here. Indeed, we urge international bodies and government organizations to follow NIST's lead. As the Framework matures, the issue of long-term governance may be revisited but at this time our companies support NIST's continued stewardship of the Framework.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Loretta Polk
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

William A. Check, Ph. D.
Senior Vice President, Science & Technology
Chief Technical Officer

Matthew J. Tooley
Vice President, Broadband Technology
Science & Technology

February 23, 2016