From: **Gretchen Lohmann**
Date: Mon, Apr 10, 2017 at 4:48 PM
Subject: NCTA Comments
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Good afternoon:

Attached are NCTA's comments in the Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity proceeding.

Please let us know if you have any questions.

Gretchen M. Lohmann
Legal Assistant
NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
Discover all that we do at ncta.com

[Attachment Copied Below]

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

In the Matter of	)
	)
Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity	))
	)
Draft Version 1.1	)

COMMENTS OF NCTA - THE INTERNET & TELEVISION ASSOCIATION

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

INTRODUCTION AND SUMMARY

The business imperatives of NCTA's member companies require them to stay on the cutting edge of developing and implementing practices and techniques for identifying and addressing cybersecurity risks and vulnerabilities. Cable companies continue to employ the NIST Cybersecurity Framework[3] as a key resource in connection with their management of cybersecurity and assessment of their cyber defense protocols and practices. The voluntary nature of the Framework has been instrumental to its adoption and use by the cable industry, providing companies with the flexibility to tailor the procedures and tools contained within the

[1] NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 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 $245 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 approximately 30 million customers.

[2] Department of Commerce, National Institute of Standards and Technology, *Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity*, FR Doc. 2017-1599, 82 Fed. Reg. 8408 (Jan. 25, 2017).

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

Framework to best comport with their particular network assets, business operations, and corporate structure. For NCTA member companies serving the bulk of the nation's cable households, many key risk management processes and cyber defense measures referenced in the Framework were already incorporated into existing business practices. For smaller companies, the Framework – in conjunction with guidance on its use released in 2015 by the Federal Communications Commission's Communications Security and Interoperability Council (CSRIC)[4/] – has served as an important tool for organizing and strengthening cybersecurity practices and processes. More broadly, the Framework has provided a common taxonomy on cybersecurity matters that facilitates communication on these issues both within individual companies and across each sector of the economy.

As NIST moves into the next stage of promoting and refining the Framework, the foundational principles of the document – collaboration with industry and voluntary adoption and usage – remain critically important. While fully embracing the utility of the Framework, cable companies reiterate their reservations regarding the value of the Framework Implementation Tiers, given the risk that this rudimentary self-evaluation mechanism may be unintentionally employed as a short-hand indicator of cyber readiness. NCTA recommends that NIST refrain from moving forward with Framework refinements that are predicated upon greater reliance on the Framework Implementation Tiers.

NCTA also recognizes that there is a strong interest in devising metrics that facilitate the evaluation of progress and outcomes on cybersecurity. As a threshold matter, NIST's effort to forge a distinction between the terms "metrics" and "measures" is apt to be more confusing than

[4/] Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report, Mar. 2015, *available at* http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf.

clarifying, and NCTA suggests that this distinction be discarded. More specifically, in accordance with the risk management orientation of the Framework as a whole, metrics should be designed to support a company's specific cybersecurity risk management performance goals and security objectives. NIST should be cautious about relying too heavily on quantifiable metrics or a "scorecard" of measures implemented. Cybersecurity is not an exact science that can be readily reduced to a quantifiable measure, and the limits of conventional quantitative metrics are exacerbated by the vast differences in risk profiles. NIST should take a risk management measurement approach that focuses on the quality of both the programs being utilized and the execution of those programs. NIST's discussion of metrics should provide more latitude and encouragement for outcome-oriented risk management process metrics and place less emphasis on the quantum of informative references or cybersecurity controls implemented. Such performance criteria would be based on business and mission goals that assess the effectiveness of security investments, programs, and strategies.

I. CABLE COMPANIES CONTINUE TO RELY UPON THE NIST FRAMEWORK AS A KEY RESOURCE IN MANAGING CYBERSECURITY RISKS

Developed in collaboration with private industry, the Cybersecurity Framework released by NIST in February 2014 is a combination of a business process document on managing cyber risk and a cyber defense tool kit. Consistent with the Executive Order and Presidential Policy Directive that launched the framework process, NIST stressed the "voluntary" nature of the Framework, noting that it is designed to use "business drivers to guide cybersecurity activities" and to "manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses."

As providers of broadband service to most American households and a significant portion of commercial businesses, securing and protecting the network is a top business priority and customer satisfaction necessity for NCTA's members. 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 Framework is a key resource for the cable industry and the overall communications sector, serving as a comprehensive guide for evaluating cyber readiness and as a compendium of effective cyber defense processes, techniques, and practices.

Emphasizing the importance of a holistic approach to cybersecurity, the Framework encourages companies to approach cybersecurity as not simply a siloed information technology (IT) or network management issue, but also as a C-suite strategic risk management issue. Its central components consist of the Framework Core, the Framework Profile, and the Framework Implementation Tiers, as well as an Appendix of Information References. Comprised of a grid that delineates cyber defense activities organized around five concurrent functions,[5/] the Framework Core identifies risk management activities and optimal cybersecurity outcomes associated with those functions. It references examples of guidance and industry-developed standards to carry out those activities and achieve those outcomes, without being prescriptive or checklist compliance-oriented. The Framework Profile aims to help identify a company's current state of cybersecurity readiness and foster progress to improved states by aligning the company's cyber resources and practices with the functions, categories and practices, and standards set forth in the Framework Core – all while balancing the needs and resources of the greater enterprise. In comparing their current and desired profiles, companies may find gaps to address in an action

[5/] The functions are defined as: **Identify** (flag and manage cybersecurity risk to systems, assets, data, and capabilities); **Protect** (implement safeguards to secure those assets); **Detect** (implement capability to monitor for, and identify, the occurrence of a cybersecurity event); **Respond** (take action to mitigate or remediate a detected cybersecurity event); and **Recover** (maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity event).

plan to reduce cyber risk, consistent with their business priorities and resources. The Framework Implementation Tiers are designed to represent the degree to which an organization's cybersecurity activities are integrated into its overall risk management process and reflect the elements and objectives set out in the Framework.[6/]

The Framework also includes a list of "Informative References" to existing standards, guidelines and practices designed to illustrate common, specific methods to achieve the outcomes associated with each subcategory. They are based on widely-known guidance frequently referenced by stakeholders during the Framework development process. Examples include standards and guidelines developed by ISO, COBIT, and NIST, but the references are not intended to be exhaustive. 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.

The cable industry has been involved in a variety of efforts designed to promote awareness and use of the Framework. NCTA's Cybersecurity Working Group, comprised of cybersecurity and technology personnel from member companies, meets regularly to share information on the latest threats, cyber defense tools, and best practices. Working Group deliberations benefit from the shared language and techniques that undergird the Framework, which facilitate discussion and understanding of different strategies and practices companies may employ while managing cyber risks consistent with the unique characteristics of their organizations.

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

[6/] As detailed below in Section II, this portion of the Framework remains of limited utility to companies seeking to assess and enhance their cyber defense capabilities.

communications companies and trade organizations, both large and small, across the industry. Cable operators also continue to participate in the DHS's Framework-based initiative, the Critical Infrastructure Cyber Community (C3) 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 worked in conjunction with CSRIC IV to produce a report aimed at highlighting those elements of the Framework best-suited for use by the communications sector. The CSRIC IV Working 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."[7/] The WG 4 Report included a risk management matrix to assist companies in adapting "the NIST Cybersecurity Framework approach to cybersecurity risk management to their own operations and networks."[8/] The WG 4 Report also contained multiple appendices tailored to each communications industry sub-sector offering "concrete guidance on how to use the Framework [to] bolster cyber readiness."[9/]

NCTA member companies have used the Framework to inform their internal gap analyses, assessing cyber risk management operations to identify practices and protocols requiring additional development or refinement. Many cable companies had implemented internal gap analyses prior to the release of the Framework, but then conducted additional

[7/] The Communications Security, Reliability and Interoperability Council IV, Working Group 4, *Cybersecurity Risk Management and Best Practices*, Final Report, at 9 (March 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[8/] *Id.* at 116.

[9/] *Id.* at 9. In addition, the cable industry has worked in conjunction with CSRIC V WG5 to produce a report on the communications sector's information sharing efforts. Information sharing is listed as one of the many Informative References in the Framework's Core. The report highlights the various sharing venues utilized by the sector, and provides a guide for companies that wish to enhance their participation in information sharing.

analyses after the Framework was adopted. Regardless of what stage of analysis the companies are in, the majority have found that the Framework's Informative References are a useful resource for addressing identified gaps.

Cable operators and other entities in the Internet ecosystem have the important job of securing their networks against adroit and innovative malicious cyber adversaries operating in a constantly-changing threat landscape. The efficacy of the NIST Framework is grounded in its recognition that there is no "one size fits all" model for addressing cybersecurity risks. The flexibility afforded by the Framework that allows companies to design and develop the best possible security solutions optimally adapted to their particular risk tolerance, network architecture, customer environment, and resources must remain a core element of any successful cybersecurity policy framework. Congress identified NIST as the ongoing facilitator of the "voluntary, consensus-based, industry-led" Framework, and in this role it should continue to ensure 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."[10/]

II. NIST SHOULD BE CAUTIOUS WITH REGARD TO REFINEMENTS THAT ARE PREDICATED UPON GREATER RELIANCE ON THE FRAMEWORK IMPLEMENTATION TIERS

NCTA members remain concerned that the Framework Implementation Tiers can be misused by insurers, regulators, and other third parties as a pedestrian ranking measure that misleadingly categorizes a company's cyber readiness. While recognizing that NIST took steps to mitigate such a result in the final adoption of Version 1.0,[11/] the draft of Version 1.1

[10/] *See* Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274 § 101(a) (as codified in 15 U.S.C. § 272(c)(15)); Framework at 1.

[11/] Framework at 9 (noting that "[t]iers do not represent maturity levels" and "progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective" and that "[s]uccessful implementation of the Framework is based upon achievement of the outcomes described in the organization's Target Profile(s) and not upon Tier determination").

potentially signals heightened emphasis on Framework Implementation Tiers that could play too large a role in Framework Profiles.

For example, the draft adds new language stating that "Tier selection and designation naturally affect Framework Profiles."[12/] But that formulation risks tainting the accuracy of the Framework Profile process by implicitly encouraging companies to produce Profile gap analyses that align with the chosen tier level. Likewise, the draft proposes adding that "the organizational state represented in an assessed Tier will indicate the likely findings of an assessed Profile, as well as inform realistic progress in addressing Profile gaps."[13/] This addition also risks turning Tier selection into the "tail that wags the dog" by implicitly encouraging gap analysis findings and progress reports that align with the selected tier level. This amplifies the concern that the emphasis on Framework Implementation Tiers prods companies toward managing their cyber defense activities with an eye toward achieving a target ranking under the Tier system, rather than focusing on their ability to respond agilely to new attack vectors and previously-unknown threats.

NIST's proposed characterization of the Framework Implementation Tiers as "qualitative" is confusing and inaccurate.[14/] The Tier scheme is apt to take on far greater significance with both internal and external audiences than the actual quality of security performance and cyber readiness of an organization. Over-emphasis on the Framework Implementation Tiers could detract from implementing and executing programs and tools that

[12/] *Framework for Improving Critical Infrastructure Cybersecurity*, Draft Version 1.1, National Institute for Standards and Technology, Jan. 10, 2017 ("Draft Version 1.1"), at 9.

[13/] Id.

[14/] See Draft Version 1.1 at 23.

actually boost cybersecurity, particularly because of the possibility of outside stakeholders looking into or even questioning an organization's self-designated Tier.

Grounded in capability maturity models that have been largely discarded for software and product development, the Framework Implementation Tiers concept is out of step with contemporary best practices for technology development programs. The rigidity of capability maturity models creates friction with continuously-evolving matters such as software development and cybersecurity. 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 turn to forward-looking Agile programming models for inspiration, rather than ranking schemes that unwittingly foster checklist compliance.[15/] The Agile model emphasizes continuous improvement of software and constant evaluation and improvement throughout the development process, and is far better-suited to the fluid nature of cyber threats and the corresponding need to quickly respond and adapt defensive measures.

The proposal to incorporate cyber supply chain risk management (SCRM) assessments into the Tier levels is likewise ill-advised. While NIST has correctly identified SCRM activities as warranting some discussion in the Framework, it is, at a minimum, premature to buttress the Tier ranking scheme with SCRM criteria. NIST should digest the feedback it obtains on its proposed discussion of SCRM in Sections 3.3 and 3.4 of the draft, and then provide companies with time to internalize whatever final recommendations are adopted for Version 1.1. The centerpiece of SCRM activity is interaction with – and responsiveness from – third parties, which

[15/] See Agile Alliance's Agile Manifesto, https://www.agilealliance.org/agile101/the-agile-manifesto/.

has the potential to introduce new complexity and uncertainty into the process of using the Framework. Accordingly, any incorporation of SCRM criteria into the Framework Implementation Tiers should take place only after companies have had experience actually employing SCRM criteria as part of their use of the Framework.[16/]

III. NIST SHOULD EMPLOY AN OUTCOME-ORIENTED RISK MANAGEMENT APPROACH TO CYBERSECURITY METRICS IN LIEU OF OVER-RELIANCE ON CONVENTIONAL QUANTITATIVE MEASURES

NIST should promote development and use of cybersecurity metrics that are designed to be outcome-oriented and aimed at supporting a company's specific performance goals and objectives.[17/] In accordance with the fundamental risk management objectives of the Framework, metrics should be geared toward assessing the efficacy of a company's cybersecurity program in relation to its underlying security objectives and business environment.

Cybersecurity risk management can be measured in the same way that an organization's other risk management programs are assessed by focusing on the quality of the process or measure adopted and implemented, an organization's adherence to its standards and objectives, the process or measure's performance in comparison to industry best practices, and the process or measure's role in – and compliance with – a company's overall security plan. Cyber risk management metrics should embody the following features:

Flexibility. Cybersecurity measurements and metrics need to be flexible, in order to match the fluid nature of cybersecurity. An organization's attack surfaces are constantly

[16/] Any SCRM recommendations within the Framework should be cabined to assets used to operate or support critical infrastructure under a company's control. It would be counterproductive – and beyond NIST's purview – for the Framework to address SCRM on an enterprise-wide or end-to-end network basis.

[17/] As noted above, NCTA believes that the effort to separately delineate "metrics" from "measures" is likely to produce confusion and error. Unless otherwise noted, we use those terms interchangeably in these comments.

changing, as are the attack vectors used by attackers. Any cybersecurity measurements and metrics used by organizations need to be designed to account for these ever-changing parameters.

Adaptability. Metrics also must be adaptable and capable of application across a variety of different organizational structures, security practices, and risk environments. The Framework is predicated upon the insight that one size does not fit all for cybersecurity, and metrics aimed at assessing a company's security performance and progress must be similarly adaptable.

Individually Tailored. Any discussion within the Framework of cybersecurity metrics must be expressly qualified to reflect the fact that all measurements are relative to an organization's self-determined risk assessment. Metrics should be aimed principally at providing a gauge of a company's internal progress on cyber readiness, rather than as benchmarks for comparison within or across sectors. Notwithstanding the value in the interconnected Internet ecosystem of developing methodologies for companies to evaluate the cyber risk management practices of potential partners and business peers, such comparative metrics across or between sectors would need to account for wide variances in security postures, organization size and scale, business models, and risk environments. NIST should proceed iteratively here, developing workable and reliable metrics for internal company use, before moving toward development of comparative measures.

Performance-Driven. In the current draft, NIST has proposed to use Implementation Tiers as one of the ways to measure an organization's cybersecurity risk management behavior. As noted in Section II, the underlying challenges of identifying quantitative, forward-looking cybersecurity metrics that are adaptable to a variety of different company structures, business models, and risk environments are exacerbated by the risk that the utility of reductive measurements like the Framework Implementation Tiers will be skewed by internal organizational biases or external pressures to achieve a predetermined tier ranking. Recommended metrics should be aimed at promoting robust and accurate assessments of a company's security program performance, and not toward achieving a pre-ordained tier ranking.

Quantity of Measures Employed Does Not Correspond to Quality of Security. The current draft posits that the "outcomes of the Framework core are the basis for a comprehensive set of cybersecurity management metrics," such that "the aggregate of these metrics equals a reduction (or not) of cybersecurity risk." But implementation of any particular quantum of security controls does not necessarily equate to greater or less cybersecurity. Therefore, it is important that any discussions of cybersecurity measurements and metrics do not suggest that implementing more security controls will reduce an organization's cybersecurity risk. The Draft Version 1.1 of the Framework, however, presumes that the "achievement of specific cybersecurity outcomes" can be quantitatively measured – which is simply not the case.[18/]

Risk management performance criteria focus principally on measuring compliance with a program's protocols and processes, the maturity and sophistication of the program, and the incremental value added to the company's overall security posture. Value-added is a key criterion that could be assessed by identifying a set of key performance indicators (KPIs) and then measuring those over time to see how they are trending. For example, a company could evaluate a new security program or tool by measuring, over a specified period before and after deployment of such program or tool, the mean time to discovery of, or recovery from, an incident that could adversely affect the confidentiality, integrity or authenticity of network information in a materially significant manner. Alternatively, a company could assess the impact of an

[18/] *See* Draft Version 1.1 at 23 (table recommending employing "measure[s]" as the means of assessing the "achievement of specific cybersecurity outcomes"); *see id.* at 21 (describing measures as "quantifiable, observable, objective data supporting metrics").

investment in a new threat intelligence capability on the number of security intrusions that are detected and deterred prior to penetrating a particular network layer.

Of course, a KPI tethered to data on the sheer number of category incidents or intrusions would have to be contextualized to reflect internal organization issues such as a change in the breadth, volume, and value information being safeguarded as well as exogenous factors such as shifts in the threat landscape and the exfiltration targets of malicious actors. But that is precisely the value of embracing risk management performance metrics over crude quantitative measures. Performance-based metrics are inherently designed to account for and reflect the unique internal circumstances of a particular organization, as well as the impact of external factors, and are not intended to be employed as short-hand means of comparatively benchmarking multiple companies' cybersecurity to rank companies across a sector.

At this stage of the Framework's life-cycle as a risk management tool, concentrating on the development and use of individually tailored and adaptable performance-based criteria is likely to be more productive than an approach based on counting incidents or security controls. There is no evidence that implementation of "more" security controls would actually reduce cybersecurity risk.[19/] Further, despite their allure of precision and universal applicability, conventional quantitative metrics are ill-suited for cybersecurity. As the Communications Sector Coordinating Council noted previously, cybersecurity is not reducible to "exact measurements such as water, temperature, or network throughput."[20]

[19/] *See* "A Threat-Driven Approach to Cyber Security", Lochkeed Martin Corporation, http://lockheedmartin.com/content/dam/lockheed/data/isgs/documents/Threat-Driven%20Approach%20whitepaper.pdf.

[20/] Letter of U.S. Communications Coordinating Sector Coordinating Council, *Current and Future States of Cybersecurity in the Digital Economy*, NIST Docket No. 160725650, at 7 (Sept. 9, 2016).

The success or failure of particular measures – such as security training, access controls, firewalls, or other security tools and practices – is difficult to quantify because of the challenges associated with pinpointing cause and effect. A company that has undertaken a broad range of new security measures may nonetheless experience a surge in cyber incidents due to actions by malicious actors that reflect changes in the threat landscape, assets targeted for exfiltration, or even a desire to test the strength of a company's reputed cybersecurity. Further, an increase in incidents may simply reflect more sophisticated intrusion detection systems and intelligence-gathering capabilities, rather than any diminution in a company's security posture. In addition, quantitative-based measures such as tracking the sheer number of controls implemented offer little comparative value, since they do not account for variances in relative states of cyber readiness or differences in risk environments. NIST should be wary of endorsing metrics that are susceptible to generating out-of-context conclusions or that would divert attention and resources toward producing expensive, time-consuming reports that offer little insight into the quality and agility of a company's cyber defense posture.

CONCLUSION

NCTA appreciates the opportunity to share the cable industry's experience with the NIST Cybersecurity Framework. We look forward to continuing our collaboration with NIST and other government agencies and industry participants to refine the Framework and promote its use as a key resource for managing cybersecurity risk.

Respectfully submitted,

/s/ Rick Chessen

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

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

Rick Chessen
Loretta Polk
NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431

April 10, 2017