ncta

The Internet & Television Association
25 Massachusetts Avenue, NW | Suite 100
Washington, DC 20001

(202) 222-2300

Rick Chessen
Senior Vice President,
Law and Regulatory Policy

o (202) 222-2445 e rchessen@ncta.com

January 19, 2018

Mr. Edwin Games
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Subject: Cybersecurity Framework Version 1.1 Draft 2

Dear Mr. Games:

NCTA - The Internet & Television Association (NCTA) hereby submits this letter in response to the request for comments from the National Institute of Standards and Technology (NIST) regarding Draft 2 of Version 1.1 of the NIST Cybersecurity Framework.[1/]

In its comments on the initial version of Version 1.1, NCTA highlighted the importance and value of the foundational principles of the Cybersecurity Framework: collaboration with industry and voluntary adoption and usage.[2/] Draft 2 helpfully reinforces this commitment, by adding new language that grounds NIST's work on the Cybersecurity Framework in the Cybersecurity Enhancement Act of 2014 (CEA).[3/] Congressional enactment of the CEA updated and codified the process by which NIST must "coordinate closely and regularly with relevant private sector personnel and entities" in a "public-private collaboration on cybersecurity" to develop the Cybersecurity Framework.[4/] This law also established "voluntary, consensus-based, industry-led" measures as the preeminent Federal policy mechanism for strengthening the cyber defenses of American companies.[5/] The revised language in Draft 2 sets forth an even firmer statutory and policy foundation for NIST's continued commitment to voluntary measures and business drivers as the key pillars undergirding its administration and evolution of the Cybersecurity Framework.

[1/] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (2nd Draft), National Institute for Standards and Technology, Dec. 5, 2017 ("Draft 2"), https://csrc.nist.gov/publications/detail/white-paper/2017/12/05/cybersecurity-framework-v11/draft.

[2/] Comments of NCTA – The Internet and Cable Association, April 10, 2017, at 2-3, 6, https://www.nist.gov/cyberframework/rfc-cybersecurity-framework-draft-version-11.

[3/] Draft 2 at 1 (all references to Draft 2 are to the "with markup" version).

[4/] *See* Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, § 101(b) (as codified in 15 U.S.C. § 272(e)).

[5/] *See id.*, § 101(a) (as codified in 15 U.S.C. § 272(c)(15)).

NCTA also concurs with NIST's decision to enlarge the range of entities covered by the Framework to include any organizations relying on technology, whether their cybersecurity focus is on information technology, industrial control systems, cyber-physical systems, or the Internet of Things.[6/] As we have explained previously,[7/] strengthening cybersecurity and resilience against malicious activity is an ecosystem-wide undertaking. Accordingly, the efficacy of policies aimed at bolstering our overall cyber defenses depends upon ecosystem-wide adoption and implementation of the risk management processes and tools embodied within the Framework.

NCTA's comments also flagged the drawbacks of revisions predicated on increased reliance upon the Framework Implementation Tiers.[8/] The Tier ranking scheme could be misinterpreted as – or worse, could develop over time into – a numerical encapsulation of an organization's cyber readiness, or could be accorded excessive weight in regulatory decisions and cyber insurance determinations. Draft 2 makes changes to the discussion of the Tiers that help address these concerns, noting specifically that "[s]uccessful implementation of the Framework is based upon achieving the outcomes described in the organization's Target Profile(s), and not upon Tier determination."[9/] This revision will help to ensure that the Tiers are treated solely as a tool for internal assessment rather than as a relative measure of an organization's overall cyber readiness. In contrast, a lack of any such assurance will undermine the value and utility of the Framework by promoting checklist compliance at the expense of tangible internal progress on risk mitigation.

NCTA's comments also urged NIST to reorient its proposed guidance on metrics, so that Framework users focus on the quality of risk management processes and security measures in relation to a company's overall security plan rather than the quantity of measures employed.[10/] Metrics that track an organization's implementation of certain controls or measures are a tool that may aid in gauging its internal progress in managing cyber risk and improving decision-making about investment priorities. But metrics should not devolve into a quantitative yardstick that over-emphasizes the sheer volume of security controls employed. Instead, they should be employed in connection with a practical, outcome-oriented approach to managing cyber risk aimed at supporting a company's specific performance goals and objectives. We applaud NIST for the changes to Section 4.0 – and specifically the emphasis on self-assessment and customizing selected measurements to align with internally-determined target objectives – as constructive changes that should benefit all Framework users.[11/] Future activities related to

[6/] Draft 2 at 2.

[7/] *See e.g.*, *Experience With the Framework for Improving Critical Infrastructure Cybersecurity,* Docket No. 140721609-4609-01, National Institute for Standards and Technology, Comments of NCTA, October 10, 2014, at 13; *Promoting Stakeholder Action Botnets and Other Automated Threats*, Docket No. 170602536-7536-01, National Telecommunications and Information Administration, Comments of NCTA, July 28, 2017, at 1-2, 23.

[8/] NCTA Comments at 7-9.

[9/] Draft 2 at 11-13.

[10/] NCTA Comments at 10-14.

[11/] Draft 2 at 26-27.

metrics that are initiated pursuant to the Roadmap should be undertaken in accordance with Draft 2's new emphasis on internal self-assessment.

Lastly, NCTA appreciates NIST's decision to revise draft 2 so that supply chain risk management (SCRM) activities are not a separately-delineated component of an organization's Tier level, but are instead folded into the External Participation element.[12/] While this revision is helpful, NCTA continues to believe that it is premature to incorporate SCRM into the Tier ranking scheme at this point.[13/] Version 1.1 provides valuable guidance on SCRM steps and processes for managing cyber risks associated with external parties.[14/] Before deciding whether and how to incorporate SCRM into the Tier selection process, NIST should provide organizations with the opportunity to internalize that guidance into their risk management practices.

NCTA appreciates NIST's continued efforts to update and enhance the Cybersecurity Framework and we look forward to continuing to collaborate with NIST on refining and improving this important resource for managing cybersecurity risk.

Sincerely,

/s/ Rick Chessen

Rick Chessen
Senior Vice President
Law & Regulatory Policy

Loretta Polk
Vice President &
Associate General Counsel

[12/] *Compare* Draft 2 at 13-15 and Draft 1 at 10-12.

[13/] NCTA Comments at 9-10.

[14/] Draft 2 at Sections 3.3, 3.4.