**Before the**
**National Institute of Standards and Technology, U.S. Department of Commerce**
**Gaithersburg, Md. 20899**

| | | |
|---|---|---|
| In the Matter of: | ) | |
| | ) | |
| Request for Comments; Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity | ) | 82 FR 8408 |


**COMMENTS OF THE AMERICAN CABLE ASSOCIATION**

## I. INTRODUCTION AND SUMMARY

The American Cable Association ("ACA") hereby submits these comments in response to the National Institute of Standards and Technology's ("NIST") Request for Comments[1] on the proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity ("Framework").[2] ACA appreciates the considerable work that NIST has put into both the original Framework and the proposed update. In particular, ACA applauds NIST's willingness to work closely with industry to develop a useful tool that "provides a common taxonomy and

[1] *Proposed Update Framework for Improving Critical Infrastructure Cybersecurity*, Request for Comment, 82 FR 8408 (rel. Jan. 15, 2017).
[2] Framework for Improving Critical Infrastructure Cybersecurity: Draft Version 1.1, National Institute of Standards and Technology (rel. Jan. 10, 2017), *available at* https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf ("Framework").

mechanism for organizations" to discuss and implement effective and comprehensive cybersecurity measures.[3]

ACA represents roughly 700 small and mid-sized cable operators, telephone companies, and municipal utilities offering broadband Internet access, video, and voice services. These operators provide service to roughly 7 million residential and commercial customers, including many anchor institutions, over networks that cover more than 18 million U.S. locations, including many in smaller towns and rural areas. Most of these providers are small with half of them serving 1,000 customers or fewer and having 10 or fewer employees. As both owners and operators of critical infrastructure, as well as small businesses whose employees live and work in the communities they serve, ACA members have considerable incentives to ensure the security of their networks. As such, they have a significant interest in the development of a cybersecurity framework that will help their businesses combat the complex and ever-changing threats they face in today's ecosystem. For these operators, the Cybersecurity Framework 1.0 has been an extremely useful tool in guiding their efforts to assess their cybersecurity vulnerabilities, and to develop and implement action plans to improve their cybersecurity posture.[4]

As it seeks to refine, clarify, and enhance the Framework, NIST should adhere to the principles that made the Framework so useful in the first place. Specifically, any updates must reinforce that the Framework is intended to be voluntary, risk-based, and flexible enough to meet the needs of a wide variety of organizations across a breadth of industries. Additionally, it

[3] *Id.* at 4.

[4] Many cable operators and other critical communications infrastructure owners and operators also use the Communications Security, Reliability, and Interoperability Council IV's Working Group 4 Report on Cybersecurity Risk Management and Best Practices, which provides further guidance on how individual companies within the Communications Sector can use and implement the NIST Framework. CSRIC IV, Working Group 4, Cybersecurity Risk Management and Best Practices, Final Report (2015), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (CSRIC IV WG 4 Report).

should continue to be clear and easy to use, especially for smaller entities that may operate with fewer resources and less expertise than their larger counterparts.

Unfortunately, many of the proposed changes contained in the Framework do not meet this standard. In particular, the proposed section on Measuring and Demonstrating Cybersecurity is confusing, and in some respects contradictory. It is not nearly ready for adoption. Rather than rush to adopt the inadequate approach to measuring cybersecurity described in Section 4, NIST should continue to work with the private sector to develop a clearer and more useful approach.

Likewise, the Framework's discussion of supply chain risk management merits further thought. The Framework should more explicitly take into account that small entities lack negotiating leverage relative to many of their suppliers and service providers, and thus have no way to influence their vendors' decision-making. In revising the Framework, NIST should recognize the limits faced by smaller entities in addressing these risks, and consider in more depth alternative steps that small business and their vendors can take to secure their supply chains.

## II. THE FRAMEWORK'S DISCUSSION OF METRICS ARE FATALLY FLAWED AND SHOULD BE REJECTED IN FAVOR OF FURTHER EXAMINATION IN COORDINATION WITH THE PRIVATE SECTOR

The Framework's proposed changes related to Measuring and Demonstrating Cybersecurity are a marked departure from the traits that make Cybersecurity Framework 1.0 so successful. Framework 1.0 clearly articulates a future-proof, technology-neutral set of principles, guidelines, and processes that an organization of any size can use to develop and implement a cybersecurity action plan. Further, it strikes an appropriate balance in describing specific risk-management practices while still providing the flexibility that organizations need to adapt the Framework to their own unique structures and missions. Any changes to the Framework should reinforce these positive traits.

Unfortunately, the proposed discussion of metrics contained in the Framework is confusing, unfocused, and in some respects contradictory. ACA appreciates the potential value of mechanisms that can help organizations measure their cybersecurity risk management, but as currently written, the discussion of metrics included in the Framework update will not help ACA's members to measure or demonstrate cybersecurity. The discussion fails to convey clear, definitional guidance, and this lack of clarity is likely to frustrate small operators and may lead some to give up on the Framework altogether. Moreover, based on the proposed changes, those that do attempt to implement the entire Framework, including its recommendations on measurement, may end up relying overmuch on a one-size-fits all checklist assessment created by third party consultants or auditors, rather than making the type of inward-looking, individualized approach to cybersecurity risk management that the Framework otherwise encourages.[5]

### A. The Discussion of Metrics Provides No Clarity As to How Cybersecurity Might Be Measured.

The Framework's overarching goal of providing a common taxonomy and mechanisms for organizations to think about cybersecurity is the right approach, but the newly added Section 4, "Measuring and Demonstrating Cybersecurity," fails to provide even a baseline understanding of what organizations should be measuring, or how they should be measuring it. Instead, it spends a considerable amount of space struggling to correlate "cybersecurity outcomes" to "business objectives."[6] Indeed, the Framework appears to view this correlation as the most essential component of measuring cybersecurity, but it also acknowledges the limitations in relying on such an approach, stating that "[t]he effect of a cybersecurity outcome on a business

[5] "The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary." Framework at 2.
[6] *Id.* at 21-22.

objective often may be unclear."[7] The updated Framework offers scant guidance in resolving this dichotomy, asserting, for instance, that "[t]he ability of an organization to determine cause-and-effect relationships between cybersecurity outcomes and business objectives also depends on the ability to adequately isolate those cybersecurity outcomes and business objectives."[8] The Framework does little, if anything, however, to provide organizations with the guidance and tools to do that. To help businesses identify and correlate cybersecurity outcomes or business objectives, the Framework does nothing more than provide a single industry-specific hypothetical example (a bank that seeks to attract online banking customers by implementing stronger authentications) to which other types of entities may not relate. This is not nearly adequate to achieve NIST's goal of providing "a common taxonomy," and it renders the discussion of metrics useless at best, particularly from the perspective of ACA members. ACA understands and certainly appreciates NIST's desire to ensure that the Framework remains flexible and cost effective, and believes that it is essential that the Framework not be prescriptive, but the Framework must strike an appropriate balance between flexibility and clarity, or else risk confusion. The proposed section on metrics does not achieve this balance.

Additionally, the Framework's discussion is inherently contradictory. It states that "[t]he objective of measuring cybersecurity is to correlate cybersecurity with business objectives, to understand and *quantify* cause-and-effect,"[9] yet the measurements and metrics described in Section 4.2 are primarily, if not entirely, *qualitative* in nature. Irrespective of the broader debate of whether quantitative metrics are an appropriate way to measure cybersecurity, or to what extent cause-and-effect can be meaningfully quantified in this area, the contradiction inherent in the Framework's discussion makes it nearly impossible to use, as any entity seeking to evaluate

[7] *Id.* at 22.
[8] *Id.*
[9] *Id.* at 21 (emphasis added).

its cybersecurity risk management practices using quantitative metrics, as suggested in the Framework, would be hard pressed to figure out what to measure or what metrics to use.

The complexity of these issues warrants further study. Instead of rushing to adopt an incomplete and confusing discussion for measuring and demonstrating cybersecurity, NIST should continue to work closely with the private sector to determine whether a useful approach can be developed that both clarifies what it means to measure and demonstrate cybersecurity, and if so, how entities might approach such measurements. This is particularly important for smaller entities, who may be less likely to know how to develop their own system of measuring cybersecurity, and thus may need to rely more heavily on the NIST Framework.

### B. The Framework's References to External Audits and Conformity Assessments Risk Creating a One-Size-Fits-All Checklist Approach to Cybersecurity.

The Framework's discussion of metrics suffers from problems other than its lack of clarity. Because Section 4.0 begins with a reference to external audits and conformity assessments,[10] it may inadvertently encourage an environment that rewards a uniform, one-size-fits all checklist approach driven by consultants and regulators, rather than the entities themselves. Framework 1.0 succeeds in providing an approach that individual entities can adapt to reflect their individual priorities and capabilities. Specifically, the Framework Profiles allow each entity to align its cybersecurity activities with its business requirements, risk tolerances and resources, while the Framework Core helps them identify the cybersecurity activities that best fit within their individual Profile.[11] The Framework Tiers then provide a mechanism for each organization to view and understand the characteristics of their approach

[10] *Id*.
[11] *Id.* at 1. ("The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources.").

to managing cybersecurity risk.[12] Updates to the Framework must maintain this approach by encouraging organizations to think of metrics in terms of internal measurements that allow them to assess the relative success and effectiveness of their own risk management processes. Some entities, particularly small businesses who lack specific expertise in this area, may elect to rely on third parties to help make that assessment, but the Framework should still explicitly encourage such entities to measure cybersecurity based on their own priorities and objectives.

Based on its efforts to couch the discussion of metrics in terms of business objectives, it appears that NIST does intend for the Framework to continue to embrace this inward-looking approach. Unfortunately, the vagueness and confusion of the discussion generally, when combined with an inferred emphasis on external audits and conformity assessments, is a near-perfect recipe for an over-reliance on check-lists based on the priorities of external actors. As NIST continues to evaluate the issue of metrics, it should view as its goal the creation of a document that will help entities develop their own measurement framework, even if they choose to engage with external third parties as a supplement to their internal review.

## III. THE FRAMEWORK'S DISCUSSION OF SUPPLY CHAIN RISK MANAGEMENT SHOULD RECOGNIZE THE MARKET REALITIES THAT PREVENT MANY ENTITIES FROM IMPLEMENTING HIGHER-LEVEL CONTROLS

The proposed updates to the Framework include the addition of Supply Chain Risk Management ("SCRM") as a component of the Framework Tiers,[13] as well as a broader discussion in Section 3.3 of how organizations can use SCRM to better manage their cybersecurity risk.[14] ACA agrees that SCRM is an essential component of cybersecurity risk management, and the proposed updates do a decent job of broadly outlining the core concerns related to SCRM and steps that some organizations can take to reduce supply chain risk.

---

[12] *Id.* ("The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.").
[13] *See id.* at 9-12.
[14] *Id.* at 16-17.

Unfortunately, the Framework fails to recognize the impact of market forces on an entity's ability to implement such activities, as small organizations typically lack the negotiating leverage to influence their vendors' cybersecurity practices.[15]

The updated Section 3 of the Framework adds two discussions related to SCRM – an expanded Section 3.3, "Communicating Cybersecurity Requirements with Stakeholders," and a brand new Section 3.4, "Buying Decisions." SCRM has also been added as a component of the Framework Implementation Tiers.

Section 3.3 now explains that "[t]he practice of communicating and verifying cybersecurity requirements among stakeholders is one aspect of [SCRM]," and that "[a] primary objective of SCRM is to identify, assess and mitigate 'products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain."[16] As currently written, this discussion presumes that entities using the Framework have the means to obtain through negotiation a vendor's use of specific, or even general, cybersecurity and risk management protocols and practices.[17] Unfortunately, this is often not the case for small entities with significantly less market power than their vendors. Thus, small entities may be well versed on cyber threats and

---

[15] This issue was raised by the American Bar Association's Cybersecurity Legal Task Force in its recent paper, "Vendor Contracting Project: Cybersecurity Checklist," which notes that "[i]f the negotiating power of either party is outsized relative to the other, responsibility and risk may not be allocated in a way that aligns rationally with the role each party will have in the transaction or the ongoing supply of the product or service." *Vendor Contracting Project: Cybersecurity Checklist*, American Bar Association, at 4 (Oct. 17, 2016), *available at* http://www.americanbar.org/content/dam/aba/images/law_national_security/Cybersecurity%20Task%20Force%20Vendor%20Contracting%20Checklist%20v%201%2010-17-2016%20cmb%20edits%20clean.pdf.

[16] Framework at 17, *citing* NIST Special Publication 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,* Boyens *et al* (April 2015) *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[17] For example, the Cyber SCRM activities described in Section 3.3 include: 1) determining cybersecurity requirements for suppliers and external partners; 2) enacting cybersecurity requirements through formal agreement; 3) communicating to suppliers and partners how those requirements will be verified and validated; 4) verifying cybersecurity requirements are met through a variety of assessments and methodologies; and 5) governing and managing the aforementioned activities. Framework at 17.

aware of specific supply chain issues with a vendor, yet still be unable to implement any of the SCRM activities outlined in Section 3.3 to address them. Their awareness and understanding of supply chain issues places them well above Tier 1,[18] but the Framework provides very little guidance as to how they can, in practice, implement policies that will move them beyond that lowest level, which limits the usefulness of this addition to the tiers. The new Framework should address this matter more explicitly in Section 3.3.

Section 3.4, on the other hand, does acknowledge the issue of unequal market power in the context of "buying decisions," but these are distinguished from SCRM transactions "in that it may not be possible to impose a set of cybersecurity requirements on the supplier."[19] The Framework's recommendation in this case is "to make the best buying decision, optimally between multiple suppliers, given a pre-decided list of cybersecurity requirements."[20] If a service or product purchased does not meet all of the organization's cybersecurity objectives, "the organization can incorporate that residual cybersecurity risk into the overall risk management of the larger environment, addressing the residual risk through other management actions."[21]

This discussion suffers once again from a lack of clarity that makes it less useful to smaller entities. For example, the Framework states that, in situations where the organization cannot impose a set of requirements on its supplier, its objective "is to make the best buying decision, optimally between multiple suppliers, given a pre-decided list of cybersecurity requirements."[22] Unfortunately, the discussion provides no insight into how a small entity might

[18] *Id.* at 10 ("*Cyber Supply Chain Risk Management* – An organization may not understand the full implications of cyber supply chain risks or have the processes in place to identify, assess and mitigate its cyber supply chain risks.").
[19] *Id.* at 18.
[20] *Id*.
[21] *Id.*
[22] *Id.*

evaluate whether a potential vendor meets their cybersecurity requirements.[23] Additionally, although the updated Framework adds a new category for SCRM (under the umbrella of the "Identify" Function), there is neither a subcategory nor corresponding informative references that relate specifically to buying decisions. If, in lieu of such references, the Framework intends for buying decisions to be folded into an entity's overall cybersecurity risk management profile, it should include some discussion as to which of the Framework's Core Functions are most likely to be affected by buying decisions, and how.

To make the Framework updates useful to small entities, ACA encourages NIST to evaluate these issues as it continues to revise the Framework, and to consider how it can best provide SCRM-related guidance that can be tailored to suit the needs of organizations of any size.

## IV. Conclusion

ACA applauds NIST's continuing work to refine and improve the cybersecurity Framework, and appreciates NIST's efforts to collaborate with industry to ensure that any changes to the Framework retain the core principles that made the Framework so useful in the first place. Unfortunately, some of the proposed changes, particularly the discussing on Measuring and Describing Cybersecurity, suffer from serious flaws and should be rejected in favor of continued study and evaluation in collaboration with industry. Additionally, NIST should consider more closely whether there are activities and processes that small entities in particular can implement to improve their supply chain risk management.

[23] *Id.*

Respectfully submitted,

Mary C. Lovejoy

Matthew M. Polka
President and Chief Executive Officer
American Cable Association
Seven Parkway Center
Suite 755
Pittsburgh, Pennsylvania 15220
(412) 922-8300

Mary C. Lovejoy
Vice President of Regulatory Affairs
Ross J. Lieberman
Senior Vice President of Government Affairs
American Cable Association
2415 39th Place, NW
Washington, DC 20007
(202) 603-1735

April 10, 2017