From: **Kevin Rupy**
Date: Fri, Apr 7, 2017 at 3:52 PM
Subject: USTelecom Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: Robert Mayer, Anthony Jones

Please see attached comments from USTelecom.

Contact the undersigned with any questions.

Thanks, Kevin

Kevin G. Rupy
Vice President, Law & Policy
USTelecom
607 14th Street, NW
Suite 400
Washington, DC 20005

[Attachment Copied Below]

Before the
Department of Commerce
National Institute of Standards and Technology
National Telecommunications and
Information Administration

In the Matter of	**)**
	)
Proposed Update to the Framework for	**)**
Improving Critical Infrastructure	**)**
Cybersecurity	**)**

COMMENTS OF THE UNITED STATES TELECOM ASSOCIATION

USTelecom[1] provides these comments to the Department of Commerce through the National Institute of Standards and Technology (NIST) in the above referenced proceeding.[2] NIST seeks comment on proposed updates to the Framework for Improving Critical Infrastructure Cybersecurity (Framework).[3] USTelecom and its member companies have long been involved in the development and implementation of the Framework, and we greatly appreciate NIST's continuing commitment to further its enhancement.

---

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks.

[2] Federal Register Notice, Request for Comments, *Developing a Framework to Improve Critical Infrastructure Cybersecurity*, 82 Fed. Reg. 8408 (January 25, 2017) (*Framework Notice*); *see also*, Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1, National Institute of Standards and Technology, January 10, 2017 (available at: https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf) (visited April 6, 2017) (*Proposed Framework*). NIST has published two versions of the *Proposed Framework*: a version with redline markups, and a version without redline markups. USTelecom citations in these comments to the *Proposed Framework* make reference to the version with redline markups.

[3] See, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014 (available at: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf) (visited April 6, 2017) (Framework).

USTelecom's members already have substantial market-based incentives to invest in, and secure critical communications infrastructure. Regardless of the type of network platform, private companies' business models are fully dependent on having a secure, resilient, always on and reliable network. Any flaw in secure and reliable infrastructures results in reputational harm and member companies losing customers and business in a highly competitive market. As a result, these companies today take substantial – and costly – measures to ensure they remain competitive and viable in today's marketplace.

The Framework has been a valuable tool for enabling industry stakeholders to voluntarily implement cost-effective approaches to ensuring implementation of robust cybersecurity measures. As it considers its proposed revisions, USTelecom encourages NIST to recognize that industry is still in a process of encouraging voluntary use of the Framework and that it should avoid complicated mechanisms that could discourage its use.

I. USTelecom and its Industry Partners Remain Committed to the Further Development and Evolution of the Cybersecurity Framework.

USTelecom and its industry partners remain committed to the further development and evolution of the Framework, and we appreciate this opportunity to comment on the changes proposed by NIST. Given the highly fluid and rapidly evolving cybersecurity landscape, ongoing updates and enhancements to the Framework are essential to ensure its continuing effectiveness.

USTelecom has played a leading in role in the development, implementation and use of the Framework, and our industry remains committed to its success. Prior and subsequent to its implementation in February 2014, USTelecom has closely worked with industry groups, associations, nonprofits, government agencies, and international standards bodies to increase awareness and adoption of the Framework. USTelecom has been instrumental in engaging a

wide diversity of stakeholders in Framework education, and the association and its members have actively participated in all of NIST's Framework-related proceedings and workshops.

Indeed, USTelecom has taken a leadership role over the last several years in cybersecurity policy discussions, convening a series of events featuring White House, government and industry officials discussing the Framework, and the latest cybersecurity concerns. These efforts were undertaken to raise industry awareness of the Framework, and to help ensure that it was be embraced by a broad range of USTelecom's member companies based on its self-evident value. As an adjunct to this work, USTelecom held eight National Cybersecurity Policy Forums between March, 2015 and December 2016 that covered a broad range of issues relating to implementation of the Framework and other national cybersecurity policy issues. Topics ranged from cybersecurity successes, challenges and goals,[4] to showcasing industry use of the Framework.[5]

Efforts such as these leveraged the ongoing close coordination by USTelecom with other state and federal agencies that were becoming involved with cybersecurity issues. USTelecom's members participate in numerous cybersecurity initiatives spread across multiple government agencies, including activities at the Department of Homeland Security (DHS) (such as DHS's Office of Cybersecurity and Communications[6] and Office of Infrastructure Protection),[7] through

---

[4] *See*, USTelecom website, *National Cybersecurity Policy Forum 2016* (available at: https://www.ustelecom.org/events-education/executive-education/national-cybersecurity-policy-forum-2016 (visited April 6, 2017).

[5] *See*, USTelecom website, *National Cybersecurity Policy Forum, Report Showcases Industry Use of NIST Framework* (available at: https://www.ustelecom.org/events-education/executive-education/national-cybersecurity-policy-forum-whats-next (visited April 6, 2017).

[6] *See*, DHS website, *Office of Cybersecurity and Communications* (available at: https://www.dhs.gov/office-cybersecurity-and-communications) (visited April 6, 2017).

[7] See, DHS website, *Office of Infrastructure Protection* (available at: https://www.dhs.gov/office-infrastructure-protection) (visited April 6, 2017).

participation in efforts involving the Communications Sector Coordinating Council (CSCC), and at the Federal Communications Commission (Commission) and its Communications Security, Reliability and Interoperability Council (CSRIC).[8]

USTelecom encourages NIST to continue to build on its successful public-private partnership model for its further development of the Framework. As highlighted in its Notice, NIST observes that the current Framework "incorporates voluntary consensus standards and industry best practices to the fullest extent possible and is consistent with voluntary international consensus-based standards."[9] USTelecom strongly encourages NIST to pursue this collaborative approach to further development of the Framework, and avoid any actions that could move it in the direction of a compliance regime with prescriptive standards leading to private sector audits and reporting.

Instead, NIST should continue to follow the successful path used during initial creation of the Framework involving collaboration with a broad range of stakeholders. Government and private stakeholders can accomplish more working through a collaborative and cooperative effort where each side brings complementary competencies, resources, and capabilities. For example, private stakeholders have valuable entrepreneurial and innovative insights that are of tremendous value to the cybersecurity effort. Additionally, these stakeholders have important insights into cybersecurity approaches that can or cannot work in a competitive marketplace. For its part, the federal government has vast resources in the form of extensive expertise, access to critical resources and a diverse and substantial user base. Ongoing collaboration between public sectors,

---

[8] *See*, Federal Communications Commission website, *Communications Security, Reliability and Interoperability Council* (available at: https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-10) (visited April 6, 2017).

[9] *Framework Notice*, p. 8409.

private sectors, and academia will continue to play a crucial role in the further development of the Framework.

II. NIST Should Proceed Cautiously on any Proposed Measurement Component.

USTelecom recognizes that there are calls across numerous government entities to measure the effectiveness of the NIST Framework. Since its release in February 2014, NIST, DHS, the FCC and their industry partners continue to promote the Framework and engage in collaborative efforts to provide important cybersecurity risk management guidance to organizations.[10] USTelecom has been a leader in many of those efforts and our industry continues to demonstrate that the Framework lends impetus to coordinated efforts among government and industry to improve critical infrastructure cybersecurity.

While USTelecom understands the desire to evaluate the effectiveness of Framework adoption, the use of metrics that evaluate effectiveness against the expense of enhancing security is not the right way to conduct such an evaluation. At the macro level, it is important for NIST and the private sector writ large to formulate a measurement approach that can be used as a reliable indicator of our nation's progress in using risk management processes to improve critical infrastructure cybersecurity.

At the enterprise level, measurements are essential to evaluate the effectiveness of cybersecurity risk management activities and plans. However, as currently presented in the update, it remains unclear how: 1) the proposed approach would provide useful insight into

---

[10] *See*, NIST website, *Cybersecurity Framework - Industry Resources* (available at: https://www.nist.gov/cyberframework/industry-resources) (visited April 7, 2017); *see also*, DHS website, Critical Infrastructure Cyber Community C³ Voluntary Program (available at: https://www.dhs.gov/ccubedvp) (visited April 7, 2017); CSRIC Final Report, *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report*, March, 2015 (available at: https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf) (visited April 7, 2017) (*CSRIC Report*).

measuring the overall effectiveness of the Framework on reducing cybersecurity risk to our nation's critical infrastructure, and 2) whether the proposed approach provides a clear value proposition for individual organizations that either do not have a measurement system in place due to, for example, resource constraints or have an existing system in place that has been shown to support their decision-making processes.

A. Any Proposed Measurement Component Must Be Consistent with the 2013 Executive Branch Guidance.

As NIST and other stakeholders contemplate the use of a measurement schema to help evaluate the success of a cybersecurity risk management plan, it is critical to the future success of the Framework that any approach remains consistent with the foundational principles upon which it was designed. Both the Executive Order that called for the Framework[11] and the initial version of the Framework[12] developed by NIST with industry collaboration speak to foundational principles that govern its implementation and subsequent development.

The Executive Order makes clear that the Framework is to incorporate "voluntary consensus standards and industry best practices to the fullest extent possible"[13] and promoted as a "voluntary" critical infrastructure cybersecurity risk management program."[14] After an eight month process with significant input from industry and other stakeholders, NIST delivered Version 1.0 which recognized that individual organizations will "continue to have unique risks –

---

[11] *See*, Executive Order, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013 (available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity) (visited April 6, 2017) (*Executive Order*).

[12] *See generally*, *Framework*.

[13] *See*, *Executive Order*, § 7(a).

[14] *Id.*, § 8.

different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the framework will vary."[15]

The NIST report emphasized that the "[F]ramework is not-a-one-size-fits-all approach to managing cybersecurity risk for critical infrastructure."[16] The fact that the Framework remained a voluntary option for organizations with its inherent flexibility and no "one-size fits all" set of expectations were key factors in gaining virtually universal support among industry for the overall project.

In reviewing the proposed updates, USTelecom is concerned that the approach proposed by NIST in Section 4.0 Measuring and Demonstrating Cybersecurity will not be cost-effective, or provide private sector companies sufficient flexibility to craft their own cybersecurity risk management assessment program. Furthermore, by devising structured metric and measurement parameters that can be explicitly used to support external audits and conformity assessments,[17] NIST risks creating a perception that the CSF will lead us down a path of compliance, benchmarking, or reporting.

B. Added Complexity to any Measurement Construct will Deter its Use by Organizations.

USTelecom is concerned that NIST offers a highly speculative proposition that organizations can effectively correlate risk management and technical control outcomes with business objectives.[18] While acknowledging that "the effect of cybersecurity outcomes on a business objective may often be unclear," NIST goes on to state that "the ability of an organization to determine cause-and-effect relationships between cybersecurity outcomes and

---

[15] *Framework*, p. 2.

[16] *Id.*

[17] *Proposed Framework*, p. 24.

[18] *Id.*, p. 21.

business objectives also depends on the ability to adequately isolate those cybersecurity outcomes and business objectives."[19]

The NIST-proposed approach to measurement presents a significant level of complexity without any corresponding assurance that it is cost-effective. In fact, the example NIST uses of a retail bank serves to accentuate the uncertainty associated with the approach.[20] NIST points out that the ability to correlate stronger authentication with increases in the number of online customers, is complicated by the fact that the outcome could be a result of other factors such as messaging, consumer demographics, and communication channels.

Many small or even mid-sized businesses will not have the resources to conduct the requisite statistical analysis to validate the type of correlations that are described in the updated material. Many of these organizations are starting to embrace the Framework in its current form, and are just beginning to understand the full implications of using the Framework to effectively manage their cybersecurity risk.

For companies that have developed their own unique approach to measure their cybersecurity performance, a new Framework overlay could be an additional layer of effort that is of marginal incremental value or potentially redundant to their current measurement review processes. Today, organizations of all sizes remain focused on addressing ever evolving cybersecurity vulnerabilities and may not have the luxury of building new or different complex data gathering and analysis functions that may be of questionable value, or even counter-productive if existing resources are misallocated.

At a minimum, NIST should forthrightly acknowledge this complexity and address the potential costs associated with implementing the proposed approach. NIST should also clarify

---

[19] *Proposed Framework*, p. 22.

[20] *Id.*, p. 21.

how its proposal will directly support our collective ability to evaluate the effectiveness of the Framework and demonstrate the business value proposition associated with statistical correlation of control and process outcomes with business results.

C. NIST Must Differentiate Between Government and Industry Use of the Framework, Especially in the Context of Measurement.

NIST has added an entirely new section on "Federal Alignment" noting that the Framework "complements existing federal risk management approaches" and federal agencies may find it to be a valuable addition to their current risk management approaches.[21] It is also becoming evident that federal government agencies are encouraged, or may be required to adopt the Framework as the overarching basis for managing their cybersecurity risk.[22] USTelecom supports any effort to improve federal agency performance in this area and we believe the framework can be effective in advancing those objectives.

We are also mindful of the need for government to measure performance across all departments and agencies and we understand why structured audits are necessary to facilitate ongoing federal compliance with good practices. However, this is not the case for the private sector where use of the Framework was deemed voluntary and intended to offer companies substantial flexibility in how it was used. We are concerned that the measurement proposal that is part of the update anticipates the need for such conformity in the federal sphere, while it ignores the potential deterrent effect it may have on private sector use and implementation.

---

[21] *Proposed Framework*, p. 20.

[22] *See*, Waterman, Shaun, CyberScoop, *Bill aims at new role in federal cybersecurity for NIST and its framework*, March 1, 2017 (available at: https://www.cyberscoop.com/bill-aims-new-role-federal-cybersecurity-nist-framework/) (visited April 7, 2017).

D. NIST Should Leverage Ongoing Industry Efforts Regarding Measurement.

In developing a Framework measurement construct, NIST can leverage the work of the communications sector which studied the area of measurement as part of a FCC CSRIC initiative to adapt the Framework to the broadband, cable, satellite, wireless and wireline segments.[23] A dedicated Working Group of 100 diverse stakeholders worked for over a year on the Framework adaptation which received widespread acclaim for applying the sector-agnostic Framework to the communications industry. A measurement working sub-group of experts was formed to provide "insight into what constitutes meaningful indicators (*i.e.*, cybersecurity metric(s)) of successful cybersecurity risk management; facilitate communication regarding the cybersecurity metrics among Internet Service Providers (ISPs); and suggest practices that companies may consider in development and incorporation of metric into their internal cybersecurity programs."[24]

The Working Group asked a fundamental question: what makes a good cybersecurity metric? It noted that "the NIST cybersecurity framework contemplates firms determining their core mission, cybersecurity threats or risks to that core mission and then developing a "profile" of internal practices and controls, pulling from the suggested practices in the Framework, to best manage those risks."[25] As an example of how a cybersecurity metric could support these efforts, the group looked at one element associated with minimizing security threats suggesting that "all employees should receive adequate information security awareness training" with a stated goal that the training be conducted on an annual basis.[26]

---

[23] *See generally, CSRIC Report*.

[24] *Id.*, p. 357.

[25] *Id.*, p. 361.

[26] *Id.*

The Working Group indicated that a quantitative risk management metric designed to support this particular business objective could track periodic status updates on the percentage of employees trained. It offered examples of information security activities that can provide data for measurement including, among others, risk assessments, penetration testing, continuous monitoring and training and awareness programs.[27] It noted that "metrics should include enterprise-level guidance and correspond to the operational priorities of the organization."[28] It further stated that "management should use measures to review performance by observing trends, identifying and prioritizing corrective actions, and directing the application of those corrective actions based on risk management factors and available resources."[29]

It specifically referenced NIST Special Publication 800-55 Revision 1 (NIST Special Publication) as an example of a good metric.[30] The NIST Special Publication identifies characteristics of good measures, and the Working Group recommended that organizations "take these under consideration in determining what constitutes a good cybersecurity metric."[31]

The Working Group provided some important perspectives on metrics and these should be considered as part of any effort to incorporate a viable and cost-effective measurement regime in the updated Version 1.1. It examined why measuring security is difficult and based their response on practitioner experience in establishing and operating security management programs. It summarized its efforts with the following four observations:

- "Cybersecurity is not an exact science and does not provide for exact measurement such as water, temperature, or network throughput. In many cases, it

---

[27] *CSRIC Report,* p. 361.
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *CSRIC Report,* p. 361.

is difficult to determine the success or failure of a given practice, or even if recommended practices are having an impact.

- Inputs, outputs, and outcomes of cybersecurity are separated in time, making authoritative measurement challenging. In other words, protective controls such as security training, access control, or firewalls are believed to work; however, it is very difficult to pinpoint cause and effect. This makes outcomes difficult to articulate and quantify.

- Correlation does not imply causation. For example, the increase in a number of attacks or incidents may simply mean that the intrusion detection and prevention systems have been updated and tuned and are registering a greater number of events which might have gone unnoticed before.

- Different organizations have different risk environments, goals for cybersecurity, and tools that they use to capture measures, and therefore comparing organizations is challenging and may not be meaningful."[32]

NIST should acknowledge these conclusions and work with industry practitioners who man the front lines to come up with an approach that aligns with the business reality. Industry is more than willing to work with NIST and other measurement experts to evolve the risk management measurement process and to consider how it can be implemented in a flexible and cost-effective manner across all sectors and across companies of varying size.

E. NIST Should Convene an Industry Initiative to Develop a Broad Consensus on a Framework Measurement Approach

NIST should reconsider the current measurement proposal and work with industry to develop an approach that can be easily integrated with an organization's current or anticipated use of the Framework. While the current language is overly complicated and somewhat disconnected from its risk management moorings, it can serve as an effective starting point for a discussion with industry and other stakeholders on how to construct an appropriate measurement regime.

---

[32] *CSRIC Report*, pp. 362 - 363.

Such an effort should begin with reaffirming NIST's commitment to the voluntary use of the Framework as a cost-effective mechanism to manage cybersecurity risk. While USTelecom agrees with NIST's statement that metrics are used to "facilitate decision making and improve performance and accountability,"[33] in the absence of strong industry buy-in, the approach presented in the update document will not lead to widespread industry adoption of the Framework measurement approach.

NIST can help ensure broad industry support for a measurement construct by facilitating the type of dialogue that characterized the development of Version 1.0. Multi-stakeholder efforts involving a wide array of companies, academic institutions, non-profits, and government agencies will make it much more likely that any revisions to the Cybersecurity Framework are broadly socialized and considered and revised consistent with broad consensus from stakeholders.

As part of this effort to engage industry in the Framework update, NIST should undertake a separate initiative to establish criteria and a mechanism to evaluate the Framework's effectiveness over an ongoing period of time. As part of that same initiative, stakeholders should also work to develop model key performance indicators that sectors and organizations can use or modify to assess their progress implementing cybersecurity risk management plans.

III. Conclusion

By demonstrating the same commitment to partnership that was so evident with the development of Version 1.0, NIST is much more likely to achieve a satisfactory outcome that industry and government can embrace. USTelecom looks forward to working with NIST to

---

[33] *See*, *Proposed Framework*, p. 21.

ensure that the Framework remains a cornerstone for cybersecurity risk management policy in the U.S. and beyond.

Respectfully submitted,
UNITED STATES TELECOM ASSOCIATION

By: _____
Kevin Rupy
Robert Mayer

607 14th Street, NW, Suite 400
Washington, D.C. 20005

April 10, 2017