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

In the Matter of	)	
	)	
Small Business Information Security:	)	DRAFT NIST IR 7621 Rev. 1
The Fundamentals	)	

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

I. INTRODUCTION AND SUMMARY

NTCA–The Rural Broadband Association[1] ("NTCA") hereby submits these comments in response to the National Institute of Standards and Technology ("NIST," or the "institute") DRAFT NIST IR 7621 Rev. 1, Small Business Information Security: The Fundamentals.

NTCA maintains a strong working relationship with NIST, and appreciates the institute's continued efforts to ensure that the Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 ("the Framework")[2] remains voluntary for critical infrastructure operators and owners. In addition, NTCA greatly appreciates NIST's interest in trying to address the needs of small businesses, and to provide streamlined, prioritized guidance to small and often resource-challenged organizations.

[1] NTCA represents nearly 900 rural rate-of-return regulated telecommunications providers. NTCA's members help put rural Americans on an equal footing with their urban neighbors by providing broadband and other telecom services in high-cost rural and remote areas of the country. All of NTCA's members are full service local exchange carriers and broadband providers, and many of its members provide wireless, cable, satellite, and long distance and other competitive services to their communities. Each member is a "rural telephone company" as defined in the Communications Act of 1934, as amended.

[2] *See* "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, NIST, rel. February 12, 2014, available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

As NTCA has noted in previous proceedings, however, the Framework is expansive and, therefore, overwhelming and difficult to digest for small businesses that lack operations and staff comparable in size and scope to larger firms.[3] As such, small communications service providers are in need of straightforward, simplified guidance with respect to how to understand and apply the Framework within their operations. Unfortunately, at a macro-level, the NIST small business fundamentals draft is overly prescriptive despite the voluntary nature of the underlying Framework. The draft guidance seems to simplify cybersecurity into a set of static security practices. This is incongruent with Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" ("the Executive Order")[4] and, as a byproduct of the Executive Order, the risk management approach espoused by the Framework. As such, the draft may send a message to other Federal agencies that the Framework can and should be simplified into a list of best practices that can be wholesale adopted into regulation. A far preferable approach is to allow organizations to perform their own individual risk assessments, and, based upon their unique threats and resultant needs, implement appropriate cybersecurity best practices as they see fit, based upon a menu of options, educational guidance, and other resources made available by the Federal government.

Working toward this end goal, the Communications Security, Reliability and Interoperability Council IV Working Group 4 ("CSRIC IV WG 4") has undertaken a collaborative initiative to develop practical, real-world guidance for communications operators,

[3] *See* Comments of NTCA, In the Matter of Request for Information, Experience with the Framework for Improving Critical Infrastructure Cybersecurity, Docket No. 140721609-4609-01 ("Comments of NTCA, RFI").

[4] *See* "Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," rel. February 19, 2013, available at: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

and, more specifically, small and mid-size businesses ("SMBs"), with regard to how they can apply the Framework to their operations. The CSRIC IV WG 4 Report, slated to be publicly released in Aril 2015 by the Federal Communications Commission ("FCC"), will offer a blueprint that other interested parties, including NIST, can adopt to develop much-needed direction and simplified guidance for small businesses, while still incorporating the risk management approach and the principles of flexibility and scalability native to the Framework.

Given the foundational issues with the NIST draft, the institute should refrain from formally publishing the document until it aligns with the flexible, risk management approach espoused by the Framework and can leverage the findings of the CSRIC IV WG 4 Report. However, if NIST would like to proceed forward with developing resources for small businesses at this point in time, it should endeavor to record real-world use cases, i.e., the myriad of ways in which a critical infrastructure operator can digest and use the Framework within its operations, and develop supporting documentation in regard to how the risk management concept can be applied to cybersecurity.

II. AT A MACRO LEVEL, THE NIST SMALL BUSINESS DRAFT IS OVERLY PRESCRIPTIVE AND, THEREFORE, INCONGRUENT WITH THE EXECUTIVE ORDER AND THE FRAMEWORK PRINCIPLES OF FLEXIBILITY AND SCALABILITY

Created through an extensive public-private partnership between NIST and industry representatives, the U.S. government has endorsed the Framework as the overarching blueprint for current and future cybersecurity efforts by critical infrastructure operators and owners.[5] In

[5] Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," advances a "national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure." Released in tandem with the Presidential Policy Directive, Executive Order 13636 calls for the development of a voluntary risk-based

turn, the Framework is built on a risk management approach to cybersecurity that enables critical infrastructure operators to identify, assess, and adequately respond to cybersecurity risk. Precise security measures and practices can vary, as a given critical infrastructure operator prioritizes the greatest risks to its business needs and functions, and then subsequently determines where and how best to apply resources to minimize, monitor, and control the probability and/or impact of potential cybersecurity events. Critical infrastructure operators of all sizes must be able to retain this flexibility in order to respond to changing marketplace demands and evolving technological capabilities, as well as cyber-based threats. As NIST noted in the Framework introduction:[6]

> 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. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

However, a prescriptive small business guide to cybersecurity would eliminate the innate agility and subsequent security advantages inherent through the use of the Framework. Unfortunately, in an admirable haste to help meet the needs of small businesses, NIST has abandoned the flexible, risk management approach that benefits large and small critical infrastructure operators alike.

Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks – and asks regulatory agencies to leverage the Framework as appropriate to mitigate cyber risk. *See* White House, Statements and Releases, "Executive Order on Improving Critical Infrastructure Cybersecurity," released February 12, 2013: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0.

[6] The Framework, page 2.

Instead, the NIST small business draft sends a message to regulators that cybersecurity can be easily simplified into a checklist of best practices. Although well meaning, the institute has included the Framework subcategories alongside the NIST draft recommendations, which, in turn, makes it possible for regulatory agencies to wholesale adopt the implicated Framework subcategories into new, unfunded mandates that may bear little relevance to a given small firm's operations or risk profile. This undermines NIST's efforts to further the Framework and its flexible, adaptable risk management approach within the Federal government.

In addition, given the nature of current threats and bad actors, a public list of common security practices is not wise. As NTCA has also noted in past proceedings,[7] attackers are becoming more and more sophisticated, and, once they are aware that a critical infrastructure operator—particularly a small, resource-challenged business—has implemented specific controls, those bad actors can revise their strategies to incorporate new methods, knowing that a carrier's resources are already tied up implementing the regulatory requirements.

It would therefore be a strategic mistake to simplify the Framework into a specific, prescribed, static set of cybersecurity best practices. Rather, a far preferable approach is to allow organizations to perform their own individual risk assessments, and, based upon their unique threats and resultant needs, implement appropriate cybersecurity best practices as they see fit, based upon a menu of options, educational guidance, and other resources made available by the Federal government, which incorporate the risk management technique and the principles of flexibility and scalability.

[7] *See* Comments of NTCA, RFI.

III. CSRIC IV WG 4 WILL OFFER VALUABLE GUIDANCE TO SMALL AND MID-SIZE BUSINESSES WITHIN THE COMMUNICATIONS SECTOR, AND A BLUEPRINT FOR NIST AND OTHER FEDERAL AGENCIES WITH RESPECT TO HOW THEY CAN DEVELOP SMALL BUSINESS GUIDANCE CONSISTENT WITH THE FRAMEWORK

As NTCA has noted in past proceedings,[8] segment-specific guidance may be able and better positioned to meet the needs of small businesses. Consistent with the multi-stakeholder collaborative approach used to create the Framework, the communications industry has convened a large working group to develop sector-specific guidance for communications operators, and, more specifically, small and mid-size communications businesses within the sector.

CSRIC IV WG 4, an advisory council to the Federal Communications Commission ("FCC"), was tasked with conforming the NIST Framework to the communications sector while maintaining flexibility for individual companies. CSRIC IV WG 4 contains more than 100 members from all segments of the communications industry. The Working Group also contains a sub-group devoted to the needs of SMBs.

Using the NIST Framework as a guide, the SMB Feeder Group adapted the Framework for its core constituency. The end product, which is currently in draft form and will be publicly available in April 2015, provides real-world, practical guidance for SMBs within the communications segment, while retaining the flexible, scalable, prioritized, and cost-effective components noted in the Executive Order, and the risk management approach native to the Framework.

The SMB report provides multiple ways for a small business to view and digest the Framework. For instance, the SMB Report includes a prioritized, culled list of Framework

[8] *Id.*

subcategories, which may be helpful as useful starting point for an SMB that is seeking to undertake a more formalized and structured risk management approach to protect its core network and critical infrastructure and services from cyber threats. The SMB Group notes that the subcategory listing is for illustrative purposes only, and should not be boiled down to an inclusive list that pre-defines which NIST Framework subcategories apply to all SMBs within the communications sector. Rather, consistent with the NIST Framework, each company should examine its network, core business objectives/mission, risk tolerance, and security needs to determine which subcategories—of the 98 included in the NIST Framework—are most applicable to its operations.

Although the culled, prioritized list may be a helpful starting point for those SMBs that are intimately familiar with the NIST Framework, others may need more substantive guidance with simplified language and recommendations. As such, the SMB Feeder Group created narratives, using the subcategories as a guide, which are centered on three basic questions: what does an SMB need to protect; who has the responsibility for a given task; and how will an SMB protect its core network and critical infrastructure and services (i.e. develop plans for identification, prevention, recovery, and continual improvement). In addition, the SMB Feeder Group developed real-world use cases, which take multiple formats and are authored by operators of various sizes.

The entirety of the SMB Feeder Group's analysis—including the illustrative subcategory listing; the "What," "Who," and "How" narratives; and the use cases—should be taken as a whole and provide SMBs with practical guidance with regard to how they can digest and apply the NIST Framework to protect their organizations' core networks and critical infrastructure and services.

The forthcoming CSRIC IV WG 4 Report will showcase that organizations may use the Framework in very different manners. In addition, the stand-alone SMB Feeder Group Report will offer a blueprint for NIST and other federal agencies with respect to how they can provide SMBs with practical guidance, while still retaining the flexibility for individual companies to use the Framework in a manner which makes sense for their unique operations and risk environments.

IV. NIST SHOULD REFRAIN FROM ISSUING THE DRAFT IN FORMAL PUBLICATION UNTIL IT CAN ALIGN WITH THE FRAMEWORK PRINCIPLES OF FLEXIBILITY AND SCALABILITY, AND INSTEAD FOCUS ITS EFFORTS ON OTHER AREAS IN WHICH SMALL BUSINESSES MAY NEED ASSISTANCE

Given the foundational issues with the NIST draft guidance for small businesses as discussed above, NIST should refrain from formally releasing the document in final publication until the institute can align the draft with the risk management approach and the principles of flexibility and scalability native to the Framework. However, if NIST moves forward and develops resources for small businesses at this point in time, it should pursue a path more comparable to that taken by CSRIC IV WG 4 and endeavor to document real-world use cases, i.e., the myriad of ways in which a critical infrastructure operator can apply the Framework within its operations.[9] As noted by various speakers at NIST outreach events, some operators are

[9] The desire for documented real-world applications, case studies, and use cases has been noted within many forums, including NIST's December 5, 2014, status update, available at: http://www.nist.gov/cyberframework/upload/nist-cybersecurity-framework-update-120514.pdf.

using the five main categories (Identify, Protect, Detect, Respond, and Recover), while others have undertaken the Framework process as initially intended and described within the document, creating a Current and Target Profile based upon the detailed 98 subcategories. These seemingly diverse ways to use the Framework are equally relevant, and offer much-needed assistance to small businesses. Likewise, the risk management approach espoused in the Framework may be new to some small businesses, as noted at recent NIST events. Small business may benefit from additional explanation with respect to what a risk management approach entails. If NIST would like to offer substantive guidance to small businesses, these are two concrete areas where it can target its efforts.

V. CONCLUSION

NTCA appreciates NIST's continuing interest in helping to meet the security needs of small business via a variety of educational resources. Although well meaning, the current small business draft document is overly prescriptive and simplifies the Framework into a static set of cybersecurity best practices. NTCA fears this may undermine NIST's and industry's collaborative efforts to position the flexible, adaptable, and scalable Framework, and its underlying risk management approach to cybersecurity, as the foundational document that a critical infrastructure operator should reference when developing or evolving its cybersecurity program.

Given the macro-level issues with the current draft, NTCA respectfully requests that NIST refrain from formalizing the document until it can incorporate the principles of flexibility and scalability native to the Framework and possibly leverage the efforts of CSRIC IV WG 4. Instead, NIST should focus its efforts on developing supporting materials as requested by industry, such as documentation explaining risk management, and recording case studies and real-world examples of Framework use.

Respectfully submitted,

By: /s/Jill Canfield
Jill Canfield
Vice President, Legal & Industry & Assistant
General Counsel
NTCA–The Rural Broadband Association
jcanfield@ntca.org

By: /s/Jesse Ward
Jesse Ward
Manager, Industry & Policy Analysis
NTCA–The Rural Broadband Association
jward@ntca.org

4121 Wilson Boulevard, 10th Floor
Arlington, VA 22203
703-351-2000 (Tel)