Before the
U.S. Department of Commerce
Washington, DC 20230

In the Matter of	)	
	)	
Securing the Information and	)	Docket No. 191119-0084
Communications Technology and Services	)	RIN 0605-AA51
Supply Chain	)	

COMMENTS OF
NTCA–THE RURAL BROADBAND ASSOCIATION

I. INTRODUCTION

NTCA–The Rural Broadband Association ("NTCA")[1] hereby responds to the invitation of the U.S. Department of Commerce ("Commerce" or "Department") to submit comments on the methods that would be used to identify, assess and address information and communications technology and services transactions that pose an undue risk to critical infrastructure.[2] Specifically, Commerce proposes to adopt regulations to implement Executive Order 13873, issued May 15, 2019, which directed Commerce to "prohibit any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or services subject to United States' jurisdiction where Commerce determines the transaction: (i)

[1] NTCA represents approximately 850 independent, community-based telecommunications companies and cooperatives and more than 400 other firms that support or are themselves engaged in the provision of communications services in the most rural portions of America. All NTCA service provider members are full service rural local exchange carriers ("RLECs") and broadband providers, and many provide fixed and mobile wireless, video, satellite and other competitive services in rural America as well.

[2] *Securing the Information and Communications Technology and Services Supply Chain*, Docket No. 191119-0084, Dept. of Commerce, Proposed rule; request for comments, 84 FR 65316 (Nov. 27, 2019) ("Notice").

involves property in which a foreign country or national has an interest; (ii) includes information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and (iii) poses certain undue risks to critical infrastructure…."[3]

NTCA's members take great pride in serving the most rural and remote areas of the nation with the rest of the world via advanced communications networks. In delivering such essential connections, NTCA and its members recognize the important cybersecurity challenges the country faces in the global supply chain. Cybersecurity is a national imperative that requires a comprehensive public-private partnership approach. To this end, NTCA and its members have previously supported, and collaborated with, federal government personnel and communications providers on a vast array of global supply chain security matters designed to protect critical services, consumers, networks and the digital economy. Furthermore, NTCA is an executive committee member and working group participant in the Department of Homeland Security's ("DHS") Information and Communications Technology ("ICT") Supply Chain Risk Management Task Force, which brings together Federal agencies and industry representatives to address supply chain security. NTCA has also hosted a variety of discussions with its members and industry representatives to discuss best practices to address the security of the telecommunications supply chain. Additionally, NTCA received awards from the National Institute of Hometown Security, funded by DHS in 2018 and again in 2019, to promote and enhance cybersecurity awareness among NTCA's members. NTCA further routinely shares cyber-threat information issued by DHS with its members when such sharing is permitted.

[3] Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," 84 Fed. Reg. 22689 (May 15, 2019).

NTCA supports Commerce's goal in this proceeding and appreciates the opportunity to provide feedback. As drafted, however, the Notice lacks the specificity needed to provide a thorough, thoughtful and helpful analysis that would assist Commerce in achieving its goal of protecting the nation's critical communications infrastructure while not "inadvertently preclud[ing] innovation or access to technology in the United States."[4] At a minimum, however, consistent with the private-public partnership approach to cybersecurity that has proven most effective to date, NTCA encourages Commerce to provide additional clarity and detail about its proposals and to seek additional industry feedback prior to issuing final rules. Specifically, NTCA suggests that Commerce seek feedback on clearly drafted proposed rules that align with the precedent established by the National Defense Authorization Act for Fiscal Year 2019 ("2019 NDAA"). Clarity in the proposed rules would provide industry with a clear path forward and ensure alignment with the 2019 NDAA, while simultaneously fulfilling Commerce's objective.

II. EFFECTIVE CYBERSECURITY PROTECTION REQUIRES A COORDINATED APPROACH AMONG FEDERAL AGENCIES.

Commerce must balance the need to protect national security with the impact any regulations would have on business – in this case, not just the business of communications providers themselves, but also the business generated by the services they provide, including e-commerce, healthcare, education, jobs and public safety.[5] Indeed, Commerce is the federal

[4] Notice at p. 5.

[5] A 2019 survey of NTCA members concluded that "rural communications providers contributed to more than 77,000 jobs in the United States and supported more than $10 billion in economic activity across a wide range of industries. For every job created by an NTCA member, almost two additional jobs were created due to the interaction with other industries served by or supported from the spending by the telecom employees." Job Creation From Rural Broadband Companies by Robert Gallardo and Indraneel

authority charged with encouraging economic growth and fostering innovation. The uncertainty created by Commerce's proposed "case-by-case" evaluation of equipment and services already in place in communications providers' networks would be very detrimental to communications providers' business.

Commerce can provide much-needed certainty while still protecting national security by aligning any rules it adopts with the 2019 NDAA and by prospectively identifying foreign adversaries, as that term is defined by the 2019 NDAA. Specifically, NTCA encourages Commerce to provide guidelines that largely mirror the restrictions contained in the 2019 NDAA, which cover equipment and services that are either a "substantial or essential component of any system, or ... critical technology as part of any system."[6] The 2019 NDAA excludes from restrictions any equipment "that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles." [7]

Prior to adopting rules intended to secure providers' networks by precluding the use of certain equipment in the ICT supply chain, Commerce should also coordinate with other agencies as applicable, including, but not limited to, DHS, the Small Business Administration and the Federal Communications Commission ("FCC"), to create a consistent, unified, approach. Furthermore, any requirement to replace equipment must be backed by clear cost recovery mechanisms that enable such replacement and include technical assistance for affected providers whose equipment has subsequently been deemed vulnerable to nation-state cyber threats.

Kumar, Aug. 2019 at p. 6, available at https://www.ntca.org/sites/default/files/documents/2019-09/Jobs%20White%20Paper.pdf.

[6] 2019 NDAA, Sec. 889(a)(1)(A), 132 Stat. at 1917.

[7] 2019 NDAA, Sec. 889(b)(3)(B), 132 Stat. at 1917.

Providing technical assistance is especially important to help further fortify affected providers' networks against cyber-based threats and ensure that subscribers' connectivity will not be at risk as a result of any rules adopted in the instant proceeding. Moreover, such financial and technical assistance is essential to smaller, rural providers that operate on extremely thin margins and must plan for network investments many years in advance. Providing funding for affected providers is also appropriate due to the fact that providers installed the equipment and services prior to the adoption of any regulations prohibiting such equipment or services, leaving providers without any notice or even expectation that the equipment or service would be subject to a "rip and replace" requirement.

While implementing rules that align with the 2019 NDAA is one critical component, NTCA further encourages Commerce to limit the definition of "a foreign adversary" to entities identified pursuant to an Act passed by Congress.[8] This will allow all communications providers the opportunity to receive advance notice of any companies that are being considered to pose a national security threat far enough in advance for providers to make modifications to their network if needed. Furthermore, aligning the definition of a foreign adversary with an act of Congress would ensure that *all* equipment and services, regardless of whether used to provide Internet service or missile defense or household electronics, are uniformly removed from United States' communications infrastructure.

[8] The FCC, for instance, has established a procedure for publicly identifying entities that pose a national security threat that includes issuing a public notice initially designating a company as a national security threat – and the basis for such a designation – followed by a 30 day period for public comments, then a "final designation" approximately 120 days later that includes the date on which the designation will take effect. *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89 et al., Report and Order, Further Notice of Proposed Rulemaking, and Order, FCC 19-121 (rel'd Nov. 26, 2019).

III. ADDITIONAL CLARITY IN THE RULES IS NECESSARY TO PROVIDE INDUSTRY A CLEAR PATH FORWARD AND ENSURE CONTINUED INVESTMENT IN COMMUNICATIONS NETWORKS.

As currently written, Commerce's proposed rules would apply to all ICT equipment and services. This combined with Commerce's proposal to evaluate equipment and services using a "case by-case, fact-specific approach" creates significant uncertainty. The Notice is unpredictable and vague, at best, and the Executive Order which Commerce has been tasked with implementing is very broad. Together, they create uncertainty and, absent a clearer definition, make it difficult for industry to ensure compliance. The consequences for an individual company that makes reasonable business and procurement decisions that are later determined to be problematic are particularly dire.

Communications providers need more detail regarding how Commerce plans to implement rules governing communications providers' networks, including the criteria Commerce will use to evaluate transactions, how often Commerce anticipates evaluating transactions, the type(s) of transactions that will be subject to review, and how Commerce will define the terms "acquisition," "importation," "transfer," and "installation" as used by the Executive Order. Regulatory certainty would be created if Commerce provides policy guidance identifying the criteria the Department will use to determine equipment and transactions pose a national security threat. Such guidance would offer communications providers at least some direction when evaluating equipment and companies with which to do business. Without these details, Commerce's action will introduce substantial uncertainty into providers' businesses. This would chill investment in ICT infrastructure due to the concern that any equipment purchased and placed in the provider's network could subsequently be deemed a national

security threat and thus be required to be removed at substantial cost and inconvenience, not only to the provider but also to those who rely on the provider's communications service.

While NTCA appreciates Commerce's goal of "not inadvertently preclud[ing] innovation or access to technology in the United States," Commerce's proposed case-by-case evaluation would have that very effect. As noted earlier, NTCA's members are small businesses that operate on extremely thin margins and must plan for network investments many years in advance. Retroactive action would be detrimental to these providers' ability to plan and budget for future deployment. Under the proposed rules, to protect themselves and their subscribers from having to unexpectedly remove equipment and services already in place, providers would need to consult with a federal agency prior to purchasing each and every type of equipment to determine whether and to what degree particular components might be permitted or precluded (as compared to being able to consult a specific, well-defined rule that offers clear guidance *a priori*). Such a process would frustrate, rather than promote, investment and innovation.

According to a 2018 NTCA member survey, 54.9% of respondents stated that regulatory uncertainty was one of the biggest challenges to widespread fiber deployment.[9] This number decreased to 43.6% in 2019,[10] due in large part to the FCC's December 2018 Universal Service Fund Order, which established clear funding amounts for providers dependent upon federal

[9] Broadband/Internet Availability Survey Report, Dec. 2018, at p. 17, available at https://www.ntca.org/sites/default/files/documents/2018-12/2018%20Broadband%20Survey%20Report_FINAL.pdf.

[10] Broadband/Internet Availability Survey Report, Dec. 2019, at p. 16, available at https://www.ntca.org/sites/default/files/documents/2019-12/2019%20Broadband%20Survey%20Report.pdf ("2019 Survey").

funds to deploy and maintain broadband service in their communities.[11] NTCA members relied on the certainty afforded by the FCC's rules to extend fiber connections to more homes and businesses and to increase the Internet connection speeds available to subscribers.[12] At a time when Congress, multiple federal agencies and state and local governments are working hard to develop rules and funding necessary to ensure every corner of the U.S. can access high-speed Internet, NTCA urges Commerce to craft clearer rules that will perpetuate this sense of certainty and enable these investments to continue.

IV. ANY RULES ADOPTED BY COMMERCE TO IMPLEMENT THE EXECUTIVE ORDER SHOULD BE APPLIED PROSPECTIVELY.

NTCA encourages Commerce to establish three methods for addressing any transactions deemed a national security threat, depending upon the level and immediacy of the threat: (1) mitigation measures; (2) replacement of equipment and services in the provider's normal course of business; and (3) expeditious removal of existing equipment and replacement with new equipment.

As a first step to evaluating equipment and services that may pose a national security threat, and prior to ordering the removal of equipment or services already installed in networks, NTCA urges Commerce to utilize DHS' criticality assessment to identify the types of transactions that meet the criteria for mitigation measures, in accordance with Commerce's proposed rule 7.103(c)(3). In the event mitigation procedures prove inadequate to fully resolve

[11] *Developing a Unified Intercarrier Compensation Regime*, CC Docket No. 01-92, Report and Order, Further Notice of Proposed Rulemaking, and Order on Reconsideration, FCC 18-176 (rel. December 13, 2018) ("*Further Notice*" or "*Report and Order*").

[12] *See* 2019 Survey at pp. 5-6 (fiber to the home is available to 63.8% of respondents' locations in 2019, compared to 58.0% in 2018, and downstream Internet speeds of 100 Mbps or greater are available to 60.8% of respondents' customer base in 2019, up from 57.3% in 2018).

the security threat, only then should providers be required to replace the equipment identified to be a threat and only in the normal course of upgrades. If. however, Commerce deems the threat imminent and the equipment therefore must be replaced quickly, Commerce should provide funds to cover the cost of removing the equipment and purchasing and installing new equipment. Furthermore, in issuing any determination, Commerce must plan for new equipment to be installed simultaneously with the removal of identified equipment to ensure subscribers continue to have access to their communications service.

Small communications providers would be especially challenged to bear the cost needed to "rip and replace" their equipment. On top of the direct costs of replacing the equipment and increased borrowing costs, rural providers could lose revenue from a variety of sources including end-user revenue during the period the network is out of service, straining already constricted resources. Their subscribers, meanwhile, would be without this critical service until the provider has installed replacement equipment. Many, if not all, subscribers cannot afford to be without their service for days or more, as they rely on the service for health care, public safety, education, jobs and much more every day.[13] Especially in smaller communities, subscribers do not have the option of choosing from multiple broadband providers. Therefore, subscribers could find themselves in the precarious position of being without their only broadband connection unexpectedly and for an undetermined amount of time.

[13] *See, e.g.*, The One-Traffic-Light Town with Some of the Fastest Internet in the U.S., by Sue Halpern, *The New Yorker* (Dec. 3, 2019) available at https://www.newyorker.com/tech/annals-of-technology/the-one-traffic-light-town-with-some-of-the-fastest-internet-in-the-us?verso=true (describing how the high-speed broadband service offered by a small provider in rural Kentucky made it possible for a local school district to establish a telemedicine connection with an area clinic allowing students to access on-call pediatricians and mental health practitioners and added several hundred jobs to the community).

Rural providers would also be especially harmed if problematic equipment or services are not clearly identified *prior to* installation. This is due the fact that not only must smaller providers often wait months to receive equipment needed to expand or maintain their networks, but also, depending on which equipment must be replaced and where it is located, weather conditions dictate that some providers have only a few months each year during which they can install certain equipment.

V. COMMERCE SHOULD CONTINUE TO COORDINATE WITH INDUSTRY AND SEEK ADDITIONAL COMMENT ON ITS PROPOSALS.

NTCA recognizes the need to take swift action to protect communications networks and appreciates Commerce's willingness to seek comment on rules that will allow communications providers to help protect the security and integrity of the nation's communications network. Protecting the services and subscribers who rely on such services from cyber attacks is critical. However, given the complexity of the issue and the substantial impact any rules adopted pursuant to this proceeding would have on communications service providers and their subscribers, NTCA urges Commerce to continue to coordinate with industry. Identifying the best methods for protecting the communications network is complex and the ramifications for providers, their subscribers, and the public are too vast and significant to needlessly create unintended and likely long-lasting consequences.

NTCA and the communications industry have a history of working collaboratively with federal officials to protect the nation's communications infrastructure. Commerce should continue to leverage the expertise and institutional contributions of these partnerships. In order to do so, NTCA urges Commerce to provide additional details in a Further Notice of Proposed Rulemaking and to seek industry feedback on those proposals, thereby allowing industry the

opportunity to comment on any areas that need further clarification or that would create unintended consequences.

VI. CONCLUSION

NTCA supports strategic steps to manage risks in our nation's communications networks; however, any rules developed in the interest of protecting national security must provide certainty to those affected by being crafted only after close coordination with other federal officials and a thorough dialogue with communications providers. Furthermore, Commerce must not overlook the need for providers to receive prospective notice of prohibited equipment and services in order to continue expanding and maintaining their networks and to ensure their subscribers are not left without much-needed services. Accordingly, NTCA respectfully submits that the time allotted for comments in the instant proceeding is insufficient to develop a full and complete record and encourages Commerce to continue developing and refining rules that will protect the nation's communications infrastructure through prospective rules that also provide financial and technical assistance to affected providers.

Respectfully submitted,

By: /s/ *Jill Canfield*
Jill Canfield
Vice President, Legal

By: /s/ *Tamber Ray*
Tamber Ray
Regulatory Counsel

4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
703-351-2000 (Tel)

January 10, 2020