Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security	)	WC Docket No. 18-89
Threats to the Communications Supply	)	
Chain Through FCC Programs	)	
	)	

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

June 1, 2018

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

I. INTRODUCTION 4

II. NTCA SUPPORTS WELL-TARGETED PROPOSALS TO ADDRESS THREATS TO THE COMMUNICATIONS SUPPLY CHAIN AND THEREBY PROTECT NATIONAL SECURITY 5

III. THE CURRENT PROPOSAL LACKS CLARITY, DEFINITION, AND COORDINATION WITH THE BROADER NATIONAL RISK-MANAGEMENT STRATEGY 7

- A. The NPRM is Overly Broad and Lacks Clarity and Foundational Definitions 7
- B. The Proposal Departs from the Established Risk-Management Approach to Supply Chain Security Otherwise Embraced by the FCC and Administration 10
- C. The Proposal Fails to Coordinate with the Broader National Strategy, Including the Simultaneous Actions of Other Federal Agencies and the Executive Branch 13

IV. THE CURRENT PROPOSAL IS OF LIMITED VALUE IN ADDRESSING AND MITIGATING SUPPLY CHAIN RISK 16

V. THE INITIAL REGULATORY FLEXIBILITY ANALYSIS IS WOEFULLY INADEQUATE 18

VI. THE PROPOSAL IS ARBITRARY, CAPRICIOUS, AND FAILS TO ADEQUATELY CONSIDER IMPACTS ON SMALL BUSINESSES 20

VII. THE FCC SHOULD ENSURE IT COORDINATES ITS ACTIONS WITH THE WHOLE OF THE FEDERAL GOVERNMENT AND TARGETS ITS PROPOSALS PROPERLY TO PROVIDE BETTER DEFINITION 22

VIII. IF THE COMMISSION MOVES FORWARD WITH ITS NPRM, IT MUST CONSIDER ALTERNATIVES THAT MINIMIZE THE BURDENS ON SMALL BUSINESSES 23

IX. CONCLUSION 25

EXECUTIVE SUMMARY

NTCA–The Rural Broadband Association ("NTCA") and its members are committed to working with Federal agencies and the administration to ensure the physical and cybersecurity of the nation's telecommunications networks. Protecting the sanctity and security of customers' information is a central and foundational tenet of a rural telecommunications provider's business. As such, NTCA and its members support well-targeted proposals to address threats to American consumers and businesses manifested through the communications supply chain.

Unfortunately, the Federal Communications Commission's ("FCC's" or the "Commission's") current proposal is overly broad and lacks clarity. It is unclear how the Commission intends to define and enforce a prospective-only ban on equipment based upon a to-be-defined threshold of national security concerns. Instead, the Notice of Proposed Rulemaking ("NPRM") poses a series of initial questions that require extensive study and discussion – more in the nature of a Notice of Inquiry than an NPRM. Without foundational information as to what the FCC proposes precisely and how it might both serve national security interests *and* affect services upon which rural Americans depend, NTCA is unable to determine if the Commission's proposal is a sensible and a prudent method to address national security risks.

The proposal is also a stark departure from the established and well-documented risk-management approach to cyber- and supply chain security embraced by the FCC and the broader administration. The NPRM fails to coordinate with the broader national strategy, including the simultaneous actions of other Federal agencies, the Executive branch, and presiding Congressional committees. Consistent with its mission to protect critical infrastructure and cybersecurity and in keeping with its congressionally identified role as the Sector Specific Agency for communications, the Department of Homeland Security has undertaken a series of

risk assessments of the communications supply chain, including a general assessment which will take place this summer and a targeted assessment of identified vulnerabilities and threats. Taken as a whole, there appears to be a much greater need for more coordination at the Federal level.

In addition, the Commission's proposal is arbitrary, capricious, and fails to adequately consider the impacts on small businesses. The Initial Regulatory Flexibility Analysis is woefully inadequate. Commission action at this stage will likely cause a ripple of unintended consequences, threatening the sustainability of networks in high-cost areas and, in the worst-case scenario, endangering the ability of the rural consumer to connect with public safety.

Irrespective of the concerns noted above, the proposal is of limited value in mitigating supply chain risk as it would narrowly apply to those networks which are supported with universal service funds, rather than the much larger universe of telecom providers that may utilize the equipment alleged to present serious risk. A country of origin ban is also arbitrary and likely insufficient to address the security of the complex and interconnected supply chain. For these reasons again, it makes more sense for the Commission to coordinate as part of a comprehensive effort on such matters, in lieu of proceeding forward alone and ahead of broader conversations ongoing now and aimed at tackling the same issues.

If the Commission determines that it must proceed forward, it should do so with prudence and thoughtful coordination. As a threshold matter, Federal agencies of proper authority and expertise should perform a detailed risk assessment of the communications supply chain to determine if credible and verified risks to the nation's security are present, and then seek to identify specific pieces of equipment which are vulnerable, based upon the component's susceptibility to hacking, its placement in the network topography, and its function. Only then should the Federal government seek to formulate a holistic, comprehensive strategy to address

verified risks to the supply chain. At a minimum, the Commission must coordinate with the whole of the Federal government and any rule must be strictly prospective only. Affected carriers should then be afforded a reasonable time period to transition to new equipment to minimize any unintended consequences on small and rural carriers and their consumers. Finally, the FCC, in collaboration with the Small Business Administration, should ensure the provision of technical and, perhaps more importantly, financial assistance for affected small businesses.

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security	)	WC Docket No. 18-89
Threats to the Communications Supply	)	
Chain Through FCC Programs	)	
	)	

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

I. INTRODUCTION

NTCA–The Rural Broadband Association ("NTCA")[1] hereby submits these comments in response to the Federal Communications Commission's ("FCC's" or the "Commission's") Notice of Proposed Rulemaking ("NPRM")[2] in the matter of protecting against national security threats to the communications supply chain through FCC programs. For the reasons stated below, NTCA supports well-targeted proposals that seek to "minimize national security threats, while avoiding putting undue burdens on small and rural communications service providers, and those living in high-cost areas where connectivity is either lacking or needs improvement."[3] NTCA urges the Commission to further refine and define its proposal, however, and seek to coordinate with the broader national risk-management strategy for supply chain security prior to taking any action in this proceeding.

[1] NTCA represents more than 800 independent, community-based telecommunications companies. All NTCA 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.

[2] Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, WC Docket No. 18-89, Notice of Proposed Rulemaking (rel. April 18, 2018) ("NPRM").

[3] NPRM, Statement of Commission Mignon L. Clyburn.

II. NTCA SUPPORTS WELL-TARGETED PROPOSALS TO ADDRESS THREATS TO THE COMMUNICATIONS SUPPLY CHAIN AND THEREBY PROTECT NATIONAL SECURITY

Small independent telecommunications providers take great pride in serving areas of the country that are often forgotten, connecting rural and remote areas of the country with the rest of the world via advanced telecommunications services. At the heart of this business mission, protecting the security and sustainability of the telecommunications network is paramount. Indeed, cybersecurity is critical to the success of a rural telco's business. To be successful and retain the confidence of its subscriber base, the rural telco must maintain a secure network capable of transmitting and receiving sensitive and personal data and information. NTCA and its members recognize the important role they play in protecting public safety and national security. Despite their size and location, small network providers take matters of national security very seriously and recognize the pressing need to secure the telecommunications supply chain against threats derived from foreign powers and bad actors, large and small alike.

Consistent with our shared commitment to network security, NTCA supports well-targeted proposals that comprehensively address verified threats to the communications supply chain. To be successful, any proffered solution should be informed by and derived from current threat intelligence and appropriately targeted to successfully mitigate observed risks.

Although NTCA's members routinely engage in risk assessments, few entities possess singular insight into the entirety of their supply chain to comprehensively address all vulnerabilities and risks. As U.S. Department of Homeland Security Secretary Kirstjen Nielsen recently noted in a speech at the RSA Conference, successfully identifying and mitigating systemic risk within the supply chain requires extensive coordination among multiple private and

public-sector partners, including government entities, technical manufacturers, and communications operators.[4]

Given the importance of this mission and the broad scope of the task at hand, NTCA welcomes (and, indeed, believes it essential to obtain) the Federal government's assistance in identifying and evaluating cyber risks and sharing timely intelligence and mitigation recommendations. To ensure that communications operators make informed decisions as to their supply chain partners based upon current and accurate information, there is a critical need for agencies of proper jurisdiction and expertise to assess credible threats and vulnerabilities inherent within the communications supply chain, and then convey this information quickly and efficiently to private-sector telecom operators. The Federal government is in a unique position to observe and evaluate physical and cyber-based threats, and then ensure that this intelligence is subsequently shared with smaller communications providers. This requires government partners with robust technical expertise, access to classified intelligence, and an established public-private partnership with industry – a role that can only be fulfilled via the cooperation and coordination of multiple Federal agencies, chief among them the Department of Homeland Security ("DHS") and intelligence agencies such as the Department of Justice ("DOJ") and Federal Bureau of Investigation ("FBI"). Indeed, DHS, DOJ and the FBI are critical partners in our shared fight to comprehensively assess and mitigate supply chain threats, consistent with the public-private partnership model espoused within President Obama's Executive Orders and used as a foundation for President Trump's cybersecurity approach reflected in his May 2017 Executive

[4] Secretary Nielsen's Remarks at the RSA Conference, rel. April 17, 2018, available at: https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference.

Order and the U.S. Department of Homeland Security Cybersecurity Strategy released May 15, 2018.[5]

At base, a successful supply chain mitigation strategy requires coordination and collaboration between industry and the Federal government to ensure policies are based upon actionable and timely threat intelligence, appropriately crafted, and narrowly targeted to properly mitigate threats. Unfortunately, as discussed below, the Commission's current high-level proposal lacks sufficient definition and detail to enable meaningful analysis or commentary, and for that reason, the FCC should "step back" and work with other Federal agencies to scope and define the relevant risks prior to presenting for further comment a more detailed and well-crafted proposal with respect to the potential barred use of universal service funds in connection with procurement of equipment presenting such risks.

III. THE CURRENT PROPOSAL LACKS CLARITY, DEFINITION, AND COORDINATION WITH THE BROADER NATIONAL RISK-MANAGEMENT STRATEGY

A. The NPRM is Overly Broad and Lacks Clarity and Foundational Definitions

The Commission's current proposal with respect to restricting the use of universal service funds for covered suppliers is overly broad. The NPRM lacks clarity and definition, introducing threshold questions that require further study and discussion, and therefore, are more appropriately suited to a preliminary Notice of Inquiry proceeding.

[5] *See* "Executive Oder 13636: Improving Critical Infrastructure Cybersecurity," rel. Feb. 12, 2013; "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience," rel. Feb. 12, 2013; "Executive Order: Promoting Private-Sector Cybersecurity Information Sharing," rel. Feb. 13, 2015; "Executive Order: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," rel. May 11, 2017; U.S Department of Homeland Security, Cybersecurity Strategy," rel. May 15, 2018.

As stated, the notice proposes a rule to prospectively prohibit "the use of USF funds to purchase equipment or services from any communications equipment or service providers identified as posing a national security risk to communications networks or the communications supply chain."[6] Although the Commission may have intended to offer for comment a bright-line rule, which is straightforward and unambiguous, in reality its application is murky at best. Given the complexity in the design and architecture of telecommunications networks, and the interconnected nature of the supply chain, a blanket restriction on equipment and service providers, even prospectively, is quite difficult to apply.

NTCA urges the Commission to proceed with prudence and thoughtful coordination to ensure suppliers of known risks are properly identified in the first instance. As the Commission notes within the NPRM, "threats to the security of our nation's communications network posed by certain communications equipment providers have long been a matter of concern in the Executive Branch and Congress."[7] However, within the NPRM, the Commission fails to provide any new information as to why this concern has reached a tipping point that mandates the use of prescriptive regulatory rulemaking authority – an action which departs from the administration's long-standing risk-management approach to cybersecurity, as discussed in detail below. In addition, the proposed rule focuses on companies rather than equipment without explaining why *all* equipment from a given vendor may present a risk. Indeed, a prohibition based upon an equipment manufacturer's country of origin is arbitrary at best. Without more specific information regarding credible threats affecting specific components, targeting all products made by a certain company is overly broad and still likely ineffectual at mitigating supply chain threats

[6] NPRM at ¶1.

[7] *Id.*

given the complex and interwoven fabric of suppliers; rather, any prohibition should be directly tied to specific pieces of equipment that are found by other agencies with core competency in such matters to present substantiated and credible national security threats.

To be clear, complete and total security is an impossibility, even with unlimited resources. Therefore, in the interest of driving to a solution that successfully mitigates supply chain risk, at base the Commission must provide clear boundaries and definitions, which are fundamentally based upon real-world observed and assessed threats and not just theoretical possibilities.

Putting aside initial questions as to how and why a supplier is identified as meeting an unidentified risk threshold, the NPRM fails to clarify if this prospective ban would apply to new hardware, new software, and/or existing software and/or hardware. In addition, it is unclear how the Commission would define and enforce a prospective-only ban regarding carriers that may have to-be-defined equipment that meets a to-be-determined threshold already deployed within their networks – equipment which was lawfully purchased and installed based upon the regulatory structure in place at the time of the investment. For instance, regarding software, a prospective limit adopted today would be tantamount to a flash-cut ban due to the need for continual upgrades and patches, and would translate to an effective immediate ban of such gear without the otherwise promised "prospective" transition.

Without this foundational information, it is difficult to determine if the Commission's proposal is a sensible and a prudent method to address national security risks. NTCA urges the Commission to further refine and define its proposal and answer these threshold questions – and only then to seek comment on such a better-defined proposal – before proceeding forward.

B. The Proposal Departs from the Established Risk-Management Approach to Supply Chain Security Embraced by the FCC and Administration

The NPRM is a stark departure from the risk-management approach to supply chain security as specified by industry best practices, other Federal agency reports, and the Commission record.

As a foundational matter, the National Institute of Standards and Technology ("NIST") maintains and evolves the Cybersecurity Framework, the pre-eminent document regarding cybersecurity risk management best practices.[8] The Cybersecurity Framework provides a risk-analysis tool for organizations to assess and mitigate cyber risks in the content of an organization's business objectives, risk tolerance, and resource constraints. The Framework was recently updated with the addition of a greatly expanded section regarding supply chain risk management ("SCRM"). As NIST notes:

> Supply chains are complex, globally distributed, and interconnected sets of resources and processes between multiple levels of organizations. Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. Given these complex and interconnected relationships, supply chain risk management (SCRM) is a critical organizational function.
>
> Cyber SCRM is the set of activities necessary to manage cybersecurity risk associated with external parties… A primary objective of cyber 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.'[9]

As such, the Cybersecurity Framework provides critical, practical guidance regarding cyber SCRM activities. Indeed, the Framework is a foundational tool that can assist companies with

[8] "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, National Institute of Standards and Technology ("NIST") (rel. April 16, 2018), available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. ("The Cybersecurity Framework").

[9] *Id.*, Section 3.3, page 16.

"governing and managing" supply chain risk including "determining cybersecurity requirements for suppliers; enacting cybersecurity requirements through formal agreement (e.g., contracts); communicating to suppliers how those cybersecurity requirements will be verified and validated, and verifying that cybersecurity requirements are met through a variety of assessment methodologies…"[10]

In multiple venues, the Commission has endorsed the use of the Cybersecurity Framework and its underlying risk management approach as a critical tool for addressing cyber risk within the communications sector. For instance, the FCC's Communications Security, Reliability and Interoperability Council ("CSRIC") Working Group 4 released its "Final Report on Cybersecurity Risk Management and Best Practices" in March 2015, which was subsequently approved and adopted by CSRIC on March 18, 2015. The Public Safety and Homeland Security Bureau sought public comment on the CSRIC IV WG4 Report and its cybersecurity risk-management recommendations, including requesting suggested alternatives to better achieve the Commission's goals.[11] However, the public record overwhelmingly supported the report's recommendations, and to date, the Commission has taken no further action in the proceeding.[12]

In addition, in the fall of 2015 the Commission charged CSRIC V with building on the prior council's work, effectively "doubling down" on its endorsement of a risk-management approach – this time to more specifically address supply chain security risks within the communications sector. CSRIC V Working Group 6 issued reports in March and September 2016, which were subsequently adopted by the advisory council. The March report

[10] *Id.*

[11] Public Notice, FCC's Public Safety and Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management and Assurance Recommendation's, PS Docket No. 15-68, DA 15-354 (rel. March 19, 2015). ("CSRIC IV Public Notice")

[12] CSRIC IV Public Notice, see Comments of NTCA, CTIA, Motorola, TIA, SIA, and WTA.

recommended voluntary recommendations and best practices to enhance the security of hardware and software in the core public communications network – principles which were designed to be accessible for organizations of all sizes.[13] And within the final September 2016 report, Working Group 6 evaluated the "best ways to provide assurances to the FCC and the public that recommended security capabilities are being implemented by network equipment vendors, and to recommend voluntary mechanisms that provide assurances to the FCC and the public that the security practices are being applied."[14] To address these concerns, CSRIC advised that supply chain risk management programs may be appropriately considered, among other topics, at the yearly in-person meetings that were initially suggested as part of CSRIC IV, Working Group 4's recommendations issued in March 2015 – meetings which would take place voluntarily between public and private stakeholders, including communications service providers and FCC representatives.[15] Further, of particular import, CSRIC recommended "against implementing any new or additional regulations to address conformity to a particular supply chain risk assessment mechanism, or any type of written attestation to the same."[16]

Taken together, the NIST Cybersecurity Framework and, as applied to the communications sector, CSRIC's follow-up reports, specify a clear path forward. "This critical, comprehensive, and collaborative body of work provides the key foundation for understanding and addressing risk to the communications sector from information and communication

[13] CSRIC V, Working Group 6 Secure Hardware and Software: Security-By-Design Working Group 6 – Final Report: Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network, March 16, 2016. ("CSRIC V WG6, March report.")

[14] CSRIC V, Working Group 6 Secure Hardware and Software: Security-By-Design Working Group 6 – Final Report: Voluntary Security-by-Design Attestation Framework for Hardware and Software Critical to the Security of the Core Communications Network, September 2016.

[15] CSRIC IV, Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report, March 2015 ("CSRIC IV WG4 Report").

[16] *Id.*

technology products and services."[17] In contrast, a prescriptive approach contemplated by the current NPRM stands as a stark departure from the Commission's longstanding support of a risk-management approach to cyber risk, and more specifically, supply chain security. As such, given the wealth of existing documents and industry best practices which recommend a risk-management approach to supply-chain security, including the FCC's advisory council reports, NTCA urges the Commission to refrain from reverting to a traditional, prescriptive regulatory structure as contemplated in the current NPRM.

C. The Proposal Fails to Coordinate with the Broader National Strategy, Including the Simultaneous Actions of Other Federal Agencies and the Executive Branch

The NPRM lacks broader discussion of how the FCC's potential actions tie to the simultaneous actions of other Federal agencies and the Executive branch administration, and therefore, the larger national strategy to address supply chain risk.

DHS is the civilian agency responsible for serving as the Sector Specific Agency for the communications sector; the DHS Office of Cybersecurity and Communications, within the National Protection and Programs Directorate, is responsible for enhancing the security, resilience, and reliability of the nation's cyber and communications infrastructure. Consistent with its mission, DHS recently initiated a series of substantive projects to evaluate supply chain risk, in collaboration with other Federal agencies. As DHS Secretary Kirstjen Nielsen revealed in an April 17, 2018, speech at the RSA Conference, the agency is engaging is a new project to "identify and mitigate systemic risk in supply chains,"[18] including single points of failure and

[17] Rural Wireless Association ex parte, pg. 4 (April 9, 2018).

[18] *See* Secretary Nielsen's Remarks at the RSA Conference, rel. April 17, 2018, available at: https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference. In addition, DHS initiated a meeting with the Executive Committee of the Communications Sector Coordinating Council on May 15, 2018.

dependencies across sectors and industries. Further, the DHS National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis has initiated two additional projects to assess the security of the telecommunications supply chain, including a general assessment of supply chain risk for hardware, software, and services used within the telecommunications industry. This general supply chain risk assessment is ongoing and slated to be completed by the end of August 2018. Last but not least, DHS has plans to undertake a more targeted risk assessment to identify specific threats, vulnerabilities, and real-world consequences related to the telecommunications industry's supply chain. To ensure an accurate and comprehensive work product, DHS is exploring the need for collaboration with intelligence agencies, so that current threat information derived from Federal agencies who have insight concerning the nature of the threat will inform their evaluation efforts.

In addition, the Department of Commerce ("DOC") has undertaken a variety of seemingly unrelated actions tied to trade negotiations and international relations which directly impact one of the industry's suppliers often cited as a cause for concern. On April 16, 2018, in response to ZTE's failure to comply with settlement of charges for violating sanctions on Iran and North Korea, the DOC announced punitive measures against the company. The agency issued a seven-year export restriction on ZTE, which effectively results in a ban on U.S. component manufacturers selling to the company.[19] Given its reliance on U.S. chip manufacturers, ZTE summarily announced that it would be suspending business operations.[20]

[19] "Secretary Ross Announces Activation of ZTE Denial Order in Response to Repeated False Statements to the U.S. Government," April 16, 2018, available at: https://www.commerce.gov/news/press-releases/2018/04/secretary-ross-announces-activation-zte-denial-order-response-repeated

[20] *See* "China's ZTE Says Main Business Operations Cease Due to U.S. Ban," Reuters, May 9, 2018, available at: https://www.reuters.com/article/us-zte-ban/chinas-zte-corp-says-main-business-operations-have-ceased-due-to-u-s-ban-idUSKBN1IA1XF.

The DOC also has been widely reported to be considering similar action against Huawei.[21] However, President Trump indicated a potential sharp change in direction on May 13, 2018, stating that he had directed Commerce Secretary Wilbur Ross to save ZTE from collapse, as the company's failure would result in the loss of too many jobs in China.[22] In addition, Congress has also expressed clear interest in addressing supply chain security concerns within the telecommunications sector while avoiding unintended consequences on small and rural network operators and their customers.[23]

Taken as a whole, there appears to be a need for more coordination at the Federal level. It is unclear how the Commission's discrete proposal to bar USF recipients from relying upon specific manufacturers ties to the many "irons in the fire," including the broader national efforts regarding national security being debated within Congress and the extensive initiatives recently undertaken by DHS to evaluate supply chain threats to the telecommunications sector. NTCA urges the Commission to, at a minimum, pause in its actions to ensure that it coordinates with other Federal agencies and the administration on a comprehensive, holistic strategy to address supply chain risk that aims to address the same kinds of equipment based upon the same detailed risk assessments by agencies with core competency and proper jurisdiction in such matters.

---

[21] *See* "Huawei Under Criminal Investigation Over Iran Sanctions," The Wall Street Journal, April 25, 2018, available at: https://www.wsj.com/articles/huawei-under-criminal-investigation-over-iran-sanctions-1524663728.

[22] President Donald J. Trump (realdonaldtrump): "President Xi of China, and I, are working together to give massive Chinese phone company, ZTE, a way to get back into business, fast. Too many jobs in China lost. Commerce Department has been instructed to get it done!" 13 May 2018, 8:01 a.m. Tweet. https://twitter.com/realdonaldtrump/status/995680316458262533

[23] *See* House Energy & Commerce Committee Subcommittee on Internet and Technology, Subcommittee on Internet & Technology, May 16, 2018 hearing, "Telecommunications, Global Competitiveness and National Security."

IV. THE CURRENT PROPOSAL IS OF LIMITED VALUE IN ADDRESSING AND MITIGATING SUPPLY CHAIN RISK

At base, the FCC's proposal seeks to prohibit universal service spending on supply chain partners that pose a risk to national security. However, irrespective of the numerous concerns raised above with the Commission's initial approach, if enacted this prohibition would only apply to a small subset of carriers which receive universal service funds to maintain or evolve communications infrastructure; other telecommunications operators which utilize private or public funding sources would not be affected or similarly prohibited from accessing and deploying what is defined as problematic supply chain partnerships. Moreover, the current proposal fails to consider the critical operations of border patrol agents on the northern and southern borders, which roam freely between U.S. network providers and those operated by neighboring countries which often rely upon Huawei equipment, a supplier frequently cited as a cause for concern related to supply chain security. Therefore, at best, the NPRM may represent only a small "finger in the dike" response, which leaves vulnerable equipment within the larger telecommunications network untouched and thus does little to mitigate in fact meaningful risk.

In addition, a country of origin ban is arbitrary and likely insufficient to address any verified and substantiated national security risks. The telecommunications supply chain is complex, interwoven, and interdependent, as it includes a series of activities such as the "development of intellectual property and standards; fabrication of components and chips; assembly and test of devices; development of software and firmware; acquisition, installation, and management of devices in operational networks; and the data and services that operate over

those networks."[24] For instance, a representative example is the Apple iPhone, wherein more than 700 suppliers from 30 countries supply components, which are derived from numerous countries and assembled in China.[25] "Only 7% of the suppliers are U.S.-based companies, including wireless chips from Qualcomm and Intel, that are actually fabricated [in] Korea and Taiwan."[26] Generally with respect to chip fabrication, Taiwan leads with over 45% of global capacity, and China is number two at 20%, while the United States only accounts for 8%.[27] In addition, software developed for American companies is often authored by non-U.S. citizens, providing opportunity for bad actors to slip malicious code into otherwise "approved" equipment.[28]

Regardless of their size or resources, network service providers have limited visibility into the entirety of hardware and software components used within a piece of equipment, and in the case of smaller operators, limited control and leverage over the security practices of suppliers. Given the nature of the threat, supply chain security can only be addressed via risk assessment and mitigation practices which seek to evaluate threats based upon current intelligence and then mitigate or manage risks to a level that is acceptable as defined by the individual company's risk tolerance, resources, and customer needs. As such, a blanket country

[24] Testimony of Dr. Charles Clancy Professor of Electrical and Computer Engineering, Virginia Tech before the House Energy and Commerce Committee, Subcommittee on Communications and Technology, Hearing on Telecommunications, Global Competitiveness, and National Security, May 16, 2018.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *For instance, see the following active job postings from Intel, Cisco, and Symantec:* https://jobs.intel.com/ShowJob/Id/1474117/Software-Development-Engineer/; https://jobs.cisco.com/jobs/ProjectDetail/Senior-Software-Engineer-Software-Development/1228376?; https://www.naukri.com/job-listings-Princ-Software-Eng-c-Win32-Chennai-Symantec-Software-India-Pvt-Ltd-Chennai-8-to-13-years-230518008993

of origin ban based upon location of the equipment manufacturer's headquarters is likely neither efficient or effective in reducing cyber risks associated with the communications supply chain.

If a substantiated, systemic risk is found to be present and associated with specific pieces of telecommunications equipment, then a more holistic approach to supply chain security would be required to adequately address national security concerns. For that reason alone, the Commission should refrain from proceeding forward with the equipment prohibitions introduced in this NPRM; rather, the FCC should seek to coordinate its efforts with other Federal agencies and the Executive branch in developing and executing a comprehensive supply chain risk-management strategy, and only then seek comment on better-developed proposals that target specific components that are determined to present risk and provide real guidance and clarity as to what "prospective" bans on such equipment may mean.

V. THE INITIAL REGULATORY FLEXIBILITY ANALYSIS IS WOEFULLY INADEQUATE

The NPRM includes an Initial Regulatory Flexibility Analysis ("IRFA"), as is required by law.[29] However, this IRFA fails to comply with the law's most basic requirements. Each IRFA is required to contain not just a description of the rules being considered and an estimate of the number of small entities to which the proposed rule will apply, but also a description of the projected compliance requirements of the proposed rule and an identification of all relevant Federal rules which may duplicate, overlap, or conflict with the proposed rule.[30] It must also describe any significant alternatives to the proposed rule which accomplish the Commission's objectives and which minimize any significant economic impact of the proposed rule on small

[29] 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601–612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[30] 5 U.S.C. § 603(b).

entities including, but not limited to, differing compliance requirements that take into account the resources available to small entities and the use of performance rather than design standards.[31] The law also requires that the IRFA describe the projected increase of cost of credit for small entities.[32]

Despite the potential substantial impact of the proposed rules on numerous small businesses, the NPRM's IRFA is no more than a perfunctory checking of the box. The Commission dedicated a mere six paragraphs to the substance of its IRFA. While the Commission seeks comment on impacts and costs, the law requires it to gather that information *prior* to proposing new rules. The Commission offers no description of the compliance requirements, no projection of the cost of credit, no description of alternatives being considered, and despite the multitude of overlapping rules and regulations in place and being considered, the Commission's one-word response to "Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules" is "None."

As it stands, the Commission indicates that it is completely lacking information about the potential substantial negative ramifications of its proposals. It asks industry to fill in its blanks not as part of an inquiry before it proposes rules, but as part of the rulemaking process (based only upon a vaguely worded, open-ended "rule"), contrary to the intent of administrative procedure law and contrary to 5 U.S.C § 603. This NPRM and its accompanying IRFA represent an example of a rush to rules without analysis.

[31] 5 U.S.C. § 603(c).

[32] 5 U.S.C. § 603(d).

VI. THE PROPOSAL IS ARBITRARY, CAPRICIOUS, AND FAILS TO ADEQUATELY CONSIDER IMPACTS ON SMALL BUSINESSES

The Commission's proposal is arbitrary and capricious. It singles out small network service providers for disfavored treatment. As proposed, the equipment prohibition would only apply to those carriers who rely upon universal service funds to offset the substantial expenses associated with network deployment and maintenance, most of whom NTCA suspects are smaller operators.

Although small and rural carriers remain steadfast in their commitment to national security, they also are advised and incented – indeed, required by the very universal service programs now at issue – to make cost-effective decisions, especially as it relates to capital investments. At the time the equipment was installed, small carriers based their decisions upon current regulations and installed equipment in good faith that the regulatory environment would not shift and suddenly revert to retroactive decisions. The Commission's proposal to prohibit the use of certain equipment suppliers *ex post facto* would make worthless significant past investments incurred in the reliance of regulation (or lack of regulation) in place at the time of purchase – equipment which was bought and used in the furtherance of universal service goals.

If adopted, the proposal would have unintended negative affects upon network providers, including small, independent telecommunications operators which depend upon universal service funds to connect the nation's highest-cost and most rural portions of the country. It would introduce significant unforeseen costs, and if these expenses could not be practically recovered from the carrier and/or its customers, the financial strain would thereby threaten the sustainability and vitality of the network operator. In the worst-case scenario, new expenses associated with the equipment prohibition and subsequent wholesale replacement may force some small carriers out of business, thereby undermining the availability and affordability of

telecommunications services in remote and rural areas of the country, including basic 9-1-1 connectivity.

The FCC's sudden change in direction also introduces substantial uncertainty into future network deployments and the equipment selection process, which directly contradicts the foundational tenets of predictability and specificity which guide universal service. According to microeconomic theory, competition causes commercial firms to develop new products, services, and technologies, which provide greater selection and better products. The greater selection typically causes lower prices for the products, compared to what the price would be if there was no competition. Therefore, if enacted, this proposal would substantially narrow the scope of products and services available to rural operators, increasing costs for remaining "approved" equipment.[33] In addition, ironically the FCC's proposed action is in direct opposition to other various cybersecurity best practices. For instance, network diversity, particularly regarding equipment, is a security best practice, while this proposal, if enacted, would result in more homogenous networks. Finally, the two Chinese suppliers referenced most often as a cause for concern, Huawei and ZTE, are key suppliers in the 5G equipment market. If U.S. operators are unable to purchase their gear, it may place the nation at a disadvantage, behind other nations in the race to deploy next-generation networks.

[33] It cannot go without observation that at a time when all are very mindful of universal service budgets, the action contemplated here would almost certainly have an adverse impact on the costs that require supporting through various elements of the Universal Service Fund.

VII. THE FCC SHOULD ENSURE IT COORDINATES ITS ACTIONS WITH THE WHOLE OF THE FEDERAL GOVERNMENT AND TARGETS ITS PROPOSALS PROPERLY TO PROVIDE BETTER DEFINITION

Despite NTCA's concerns noted above, if the Commission determines that it must proceed forward, it should do so with abundant caution. As an initial threshold matter, Federal agencies of proper authority and expertise should perform a detailed risk assessment of the telecommunications supply chain to determine if verified, substantiated risks to the nation's security are present. If threats are found to exist, then the Federal government should seek to identify *specific pieces of equipment* which are vulnerable, matched with information about the consequence and its likelihood or probability of occurrence. Among other items, Federal agencies should consider whether the specific component is susceptible to hacking; its placement in the network topography; and its function within the network, including if it contains intelligent components. As discussed above, DHS, in collaboration with intelligence agencies, is well positioned to lead this activity and the agency already has endeavored to undertake a series of risk assessments of the communication's supply chain security.

If verified threats are found to be present and associated with specific pieces of telecommunications equipment, then a holistic approach to supply chain security would be required to adequately address national security concerns. Indeed, if nation-state threats arise, then a broad national strategy is required to successfully mitigate threats to America's telecommunications networks – a strategy which extends far beyond the limited universe of operators which receive universal service support for communications services in key areas. Further, a ban on telecommunications gear imported from other countries, even prospectively, has economic, geopolitical, and trade ramifications, which must be evaluated and reviewed at a national level.

At a minimum, to successfully address national security risks, the Commission must ensure that it coordinates its efforts with the whole of the Federal government, including other Federal agencies who have applicable expertise such as DHS, DOC, and intelligence agencies such as the FBI. Only after such coordination should the FCC seek to contemplate targeted action to address any gaps or tackle more specific issues as they relate to telecommunications network service providers.

VIII. IF THE COMMISSION MOVES FORWARD WITH ITS NPRM, IT MUST CONSIDER ALTERNATIVES THAT MINIMIZE THE BURDENS ON SMALL BUSINESSES

If the Commission determines that it must proceed forward, it should consider alternatives to its proposals that mitigate and minimize the harms to small businesses. For example, it should seek to focus on specific pieces of infrastructure which pose national security threats, as identified by agencies of expertise and authority as noted above. Further, any rule or ban must be prospective only. Network equipment has an extended lifespan, and this must be addressed and planned for in any NPRM which seeks to prospectively prohibit the use of universal funds for restricted suppliers. Affected carriers should be afforded a reasonable time period to transition to new equipment to minimize any unintended consequences posed on small and rural carriers and their consumers. For those companies that have embedded technology which is identified to fall within the to-be-defined restricted categories, network equipment cannot be summarily removed and replaced overnight – despite an operator's best efforts and an unequivocal commitment to network security. Rather, replacement equipment must be evaluated, selected, tested, deployed, and perhaps most importantly, paid for – a process that could take years, especially in extremely high-cost areas. As such, small providers, at a

minimum, should be afforded a five-year transition period which is tied to the economic or useful life of the specific, identified equipment.

During this transition period, existing hardware and software will need to be maintained, patched, and repaired, or a telecommunications operator risks jeopardizing the quality of service it provides to its customers. Affected providers should be explicitly allowed to replace failing equipment, as required, with spare parts, including procuring additional spares as needed. Equipment and software also need to be patched on a regular basis. Ironically, if systems are not regularly patched, this poses a security risk by itself as out-of-date software is highly vulnerable to cyber-attack. As such, during the transition process, software updates also should be explicitly allowed. Similarly, multi-year contracts or service agreements should last for as long as the related equipment is permitted and should be explicitly grandfathered, or a clear change of law is required.

Finally, if the Commission determines it is necessary to move with more haste, than the FCC, in collaboration with the Small Business Administration, should ensure the provision of technical and, perhaps more importantly, financial assistance for affected small businesses. As previously discussed, NTCA's small and rural members operate on extremely thin margins and must plan for network investments many years in advance. Any new, wholesale replacement of infrastructure and equipment must be supported with clear recovery mechanisms to ensure rural carriers are afforded the necessary assistance before, during, and after the transition period if national security considerations dictate anything more than an "organic" transition away from such elements at the end of their useful life.

IX. CONCLUSION

For the aforementioned reasons, NTCA urges the Commission to refrain from proceeding forward until it has engaged in further study, discussion, and coordination with other Federal agencies and the administration, and to then present more detailed, well-defined proposals for consideration should it find that any rule remains necessary in the wake of or in conjunction with broader efforts.

Respectfully submitted,

By: /s/ Michael R. Romano
Michael R. Romano
Senior Vice President – Industry Affairs & Business Development
mromano@ntca.org

By: /s/ Jill Canfield
Jill Canfield
Vice President, Legal & Industry and Assistant General Counsel
jcanfield@ntca.org

By: /s/ Jesse Ward
Jesse Ward
Director, Industry & Policy Analysis

4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
jcanfield@ntca.org
703-351-2000

June 1, 2018