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	)	

REPLY COMMENTS OF COMPETITIVE CARRIERS ASSOCIATION, THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION, ITTA – THE VOICE OF AMERICA'S BROADBAND PROVIDERS, AND NTCA—THE RURAL BROADBAND ASSOCIATION

Matt Schruers
Vice President, Law & Policy
John A. Howes, Jr.
Policy Counsel
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION
655 15th Street, NW, Suite 410
Washington, DC 20005
(202) 783-0070
www.ccianet.org

Steven K. Berry
President & CEO
Rebecca Murphy Thompson
EVP & General Counsel
Courtney Neville
Associate General Counsel
COMPETITIVE CARRIERS ASSOCIATION
601 New Jersey Avenue, NW, Suite 820
Washington, DC 20001
(202) 449-9866
www.ccamobile.org

Genevieve Morelli
President
Michael J. Jacobs
Vice President, Regulatory Affairs
ITTA – THE VOICE OF AMERICA'S BROADBAND PROVIDERS
1101 Vermont Avenue, NW, Suite 501
Washington, DC 20005
(202) 898-1520
www.itta.us

Theodore B. Olson
Thomas H. Dupree Jr.
Andrew G.I. Kilberg
Counsel for Competitive Carriers Association
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, NW
Washington, DC 20036
(202) 955-8500
www.gibsondunn.com

Michael R. Romano
Senior Vice President – Industry Affairs & Business Development
NTCA—The Rural Broadband Association
4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
(703) 351-2016
www.ntca.org

July 2, 2018

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

REPLY COMMENTS OF COMPETITIVE CARRIERS ASSOCIATION, THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION, ITTA – THE VOICE OF AMERICA'S BROADBAND PROVIDERS, AND NTCA—THE RURAL BROADBAND ASSOCIATION

I. Introduction and Executive Summary.

Competitive Carriers Association ("CCA"),[1] the Computer & Communications Industry Association ("CCIA"), ITTA – The Voice of America's Broadband Providers ("ITTA"), and NTCA—The Rural Broadband Association ("NTCA") (collectively, "the Associations") submit these reply comments in response to initial comments regarding the Federal Communications Commission's ("FCC's") proposed rule to prohibit the use of money distributed from the Universal Service Fund ("USF") "to purchase or obtain any equipment or services produced or provided by any company posing a national security threat to the integrity of communications

[1] CCA is the leading association for competitive wireless providers and stakeholders across the United States. CCA's membership includes nearly 100 competitive wireless providers ranging from small, rural carriers serving fewer than 5,000 subscribers to regional and national providers serving millions of customers. CCA also represents associate members consisting of small businesses, vendors, and suppliers that provide products and services throughout the mobile communications supply chain.

(Cont'd on next page)

networks or the communications supply chain."[2] Each of the Associations filed initial comments on this proposed rulemaking.[3]

The Associations understand the importance of protecting the United States' telecommunications supply chain from malicious actors. The proposed rule, however, is not the answer. As many commenters, including those who generally support the FCC's actions in this area, have explained, this problem can only be solved through a whole-government approach that addresses the overall telecommunications network.[4]

The proposed rule goes well beyond the FCC's core jurisdiction and the subject matter fits far better within the core competency of other agencies. As the Telecommunications Industry Association ("TIA") notes, the FCC "must balance practical considerations,

---

[2] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Notice of Proposed Rulemaking, FCC 18-42, WC Docket No. 18-89, Appendix A (rel. Apr. 18, 2018) ("NPRM").

[3] Comments of Competitive Carriers Ass'n, WC Docket No. 18-89 (filed June 1, 2018) ("CCA Comments"); Comments of the Comput. & Commc'ns Indus. Ass'n, WC Docket No. 18-89 (filed June 1, 2018) ("CCIA Comments"); Comments of ITTA – The Voice of Am.'s Broadband Providers, WC Docket 18-89 (filed June 1, 2018) ("ITTA Comments"); Comments of NTCA—The Rural Broadband Ass'n, WC Docket No. 18-89 (filed June 1, 2018) ("NCTA Comments").

[4] *See, e.g.*, CCIA Comments at 6 ("Ultimately, CCIA believes that the Commission should coordinate its efforts across all Federal Government initiatives to create a more comprehensive policy, allowing other agencies with expertise to weigh in and help ensure that there are not competing or conflicting 'blacklists.'"); Comments of Puerto Rico Tel. Co., Inc., WC Docket No. 18-89, at 6 (filed June 1, 2018) ("Puerto Rico Tel. Co. Comments") ("Given the complexity and sensitivity of the issues being addressed by the Administration and Congress, and that the Commission's expertise and resources on these matters are limited, development of a whole of government strategy would be more prudent than piecemeal measures."); Comments of the Telecomms. Indus. Ass'n, WC Docket No. 18-89, at 4 (filed June 1, 2018) ("TIA Comments") ("[T]he agency's actions should be informed by a long-term view that would ultimately require actions across the federal government."); Comments of USTelecom – the Broadband Ass'n, WC Docket No. 18-89, at 8 (filed June 1, 2018) ("USTelecom Comments") ("[T]he Commission must be involved in a coordinated fashion across the federal government in order to make an informed decision on how to best identify meaningful supply chain risks and the appropriate actions to mitigate them.").

(Cont'd on next page)

effectiveness in promoting security goals, the reality of the global ICT [information and communications technology] supply chain, and the significant repercussions its actions will likely have around the world."[5] In fact, the proposed rule is impractical, ineffective in serving its intended purpose, disconnected from the reality of the supply chain, and untethered to the agency's typical role. The proposed rule will devastate impacted rural carriers, which execute the FCC's mission to expand high-quality access to telecommunications and information services. It would harm rural consumers, with little to no corresponding benefit. In light of the very serious policy considerations and the proposed rule's dubious legality, the FCC should defer to Congress and other expert agencies before proceeding with this rulemaking.

If the FCC chooses to move forward with the rulemaking, it should at a minimum (1) provide an extended period for providers to come into compliance, (2) grandfather existing equipment and the services necessary to maintain and upgrade that equipment, and (3) offer adequate transitional funding to adversely affected carriers, along with other mitigation provisions. At the very least, the FCC needs to make a reasonable decision based on informed, public input; it thus should issue a more detailed proposed rule for further comment.

II. The FCC Should Defer to Congress and Other Expert Agencies.

The comments submitted in response to the NPRM uniformly agree that cybersecurity and supply chain management must be comprehensive.[6] The proposed regulation targets USF-funded networks and, therefore, addresses just a small fraction of the nationwide and, indeed, worldwide telecommunications network and the supply chain that feeds it. Cybersecurity is a complex issue that encompasses much more than USF-funded wireless and wireline networks

---

5 TIA Comments at 28.

6 *See supra* note 4.

and stretches far beyond the FCC's jurisdiction. The proposed rule in and of itself does little to solve the serious and interwoven cybersecurity challenges affecting American networks. Yet, the FCC's proposed rule will immediately complicate international trade and diplomacy and will have "significant repercussions . . . around the world"[7] without yielding material improvement in the United States' national security posture. The proposed rule also could result in "a compliance nightmare" as various agencies and government entities rush to keep up and implement "[i]nconsistent definitions" and policies.[8] The FCC's promulgation of a final rule targeting USF recipients will undermine careful, consistent, and collaborative regulatory action among other governmental bodies. It would be imprudent for the FCC to "plow[ ] new ground."[9]

A. Congress and Other Agencies Are Better Suited to Address Supply Chain Security.

It is more appropriate for Congress and other federal agencies to oversee security of the global supply chain. Congress has the requisite authority and a broader perspective than the FCC. The FCC could continue to have an important role in cybersecurity efforts, including with respect to the supply chain for network equipment. But Congress has advantages over the FCC in at least four areas that would allow it to more appropriately address supply chain security.

- Broad Jurisdiction. Congress enjoys broad legislative power, whereas the FCC's authority is narrow and obtained only via delegation by Congress. Congress can enact comprehensive legislation that addresses all aspects of the supply chain for

---

7 TIA Comments at 28.

8 *Id.* at 47; *see also* Comments of AT&T Servs., Inc., WC Docket No. 18-89, at 3–4 (filed June 1, 2018) ("AT&T Comments") (stressing importance of regulatory consistency for the telecommunications industry).

9 TIA Comments at 60.

(Cont'd on next page)

equipment and services that can impact cybersecurity in networks and devices, including the Internet of Things. Congress has the constitutional authority to establish an interagency framework or process through which multiple agencies with different expertise and relevant jurisdiction work together to identify and eliminate unacceptable security risks.[10] TIA has made the case for such an interagency process specifically "empowered to make national security determinations on behalf of the entire (non-military) federal government."[11] The FCC does not have the authority to "empower[ ]" federal agencies in this way, and it should not "adopt a forward-looking approach" that presumes to know what Congress may do.[12]

- Scope of Risk. Congress is better positioned to assess the risk posed by the supply chain across industrial and economic sectors nationally and globally. Congressional committees can draw upon their own expertise and the research and knowledge of numerous relevant federal agencies, including the Department of Commerce ("DoC"), the Department of Homeland Security ("DHS"), the National Security Agency, the Department of Defense ("DoD"), and other agencies in the intelligence community. In addition, Congressional committees can hold hearings to convene panels of private sector experts, as the House Energy and Commerce Committee's Subcommittee on Communications and Technology recently did.[13]

---

[10] *See, e.g.*, *infra* 7–8 & n.20 (discussing the Federal Acquisition Supply Chain Act of 2018).

[11] TIA Comments at 80.

[12] *Id.*

[13] *Hearing Before the H. Comm. on Energy & Commerce Subcomm. on Commc'ns & Tech.*, 115th Cong. (May 16, 2018).

- Costs and Benefits. Congress also is better positioned to assess the full costs and benefits of regulating the supply chain and to minimize costs across all industries and sectors, which otherwise will ultimately be borne by consumers. Congress can appropriate funds to compensate for economic injury caused by the new ground rules for the supply chain.
- Effects on Trade and Diplomacy. The premise of the proposed rule is that certain foreign companies might present particular security risks to American networks. By its very nature, the proposed rule implicates multifaceted foreign policy concerns, touching trade and diplomatic spheres that are generally not the FCC's expertise. Congress, on the other hand, can appropriately balance supply chain risks with potentially countervailing trade and diplomatic concerns. In addition to the agencies noted above, Congress may call upon the expertise of the State Department and the United States Trade Representative.

Other government agencies also are better able to address cybersecurity issues arising from the global equipment supply chain and "are much better positioned" to make the "complex technical assessments" that are necessary to determine "whether products from a particular . . . supplier pose a heightened risk."[14] For example, DHS is likely in a better position to make both the technical and national security determinations necessary to regulate effectively. As USTelecom notes, the FCC "has not previously demonstrated an independent capability to examine and evaluate technical vulnerabilities in the communications supply chain."[15] Nor is the

[14] TIA Comments at 59.

[15] USTelecom Comments at 9. Further, in response to cybersecurity portions of the FCC's 2016 Spectrum Frontiers *Report and Order and Further Notice of Proposed Rulemaking*, then-Commissioner Ajit Pai noted in a statement that the FCC "lack[s] the expertise and authority to

(Cont'd on next page)

FCC best positioned to situate those technical assessments "in the appropriate geopolitical context."[16] The simple "reality is that the Commission has far less expertise on national security matters . . . than do other federal departments or agencies."[17] Action by the FCC would be a momentous step to take before other, better equipped agencies can address the alleged supply chain vulnerability. The federal government should speak with one clear voice to effectuate the policy direction on supply chain issues rather than take a fragmented approach.

Indeed, Congress, the President, and other agencies and organizations are actively considering supply chain security matters. The House and Senate passed different versions of the National Defense Authorization Act ("NDAA") while this rulemaking has remained pending. The House bill prohibits federal agencies from purchasing telecommunications equipment and services from Huawei and ZTE, and from contracting with entities that use telecommunications equipment and services provided by Huawei and ZTE.[18] The legislation also instructs the Director of National Intelligence to study the risks posed by Huawei and ZTE and to "share such report . . . with U.S. allies, partners, and U.S. cleared defense contractors and telecommunications services providers."[19] Moreover, just a few weeks ago, Senators Lankford and McCaskill introduced another bill that would establish a Federal Acquisition Security

---

dive headlong into this issue . . . . These are issues that are better left for security experts to handle in a more comprehensive way." Statement of Commissioner Ajit Pai, GN Docket No. 14-177 (rel. July 14, 2016), *available at* https://www.fcc.gov/document/spectrum-frontiers-ro-and-fnprm/pai-statement.

[16] TIA Comments at 59.

[17] ITTA Comments at 3.

[18] John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong. § 880(b) (2018).

[19] *Id.* § 880(c).

(Cont'd on next page)

Council ("FASC") composed of representatives from various federal agencies. The FASC would be empowered to develop criteria, processes, and standards for assessing and managing supply chain risks from acquiring information technology and to coordinate the approaches to supply chain security by different agencies. The FASC also would be required to develop a strategic plan regarding supply chain risks. Furthermore, the bill specifically allows agencies to ban contracts with a company for certain procurement purposes if the agency determines that the company poses a national security threat.[20] Meanwhile, DHS is in the midst of a comprehensive risk assessment of telecommunications supply chain security, and the FCC's own Communications Security, Reliability and Interoperability Council ("CSRIC") continues to review these issues and build upon its prior work and recommendations.[21] The FCC should be informed by CSRIC's review before acting.

B. The FCC Should Stay Its Hand Pending Action by Congress or by Other Agencies.

In light of the ongoing developments discussed above, the FCC should withdraw the proposed rule. Precipitous FCC action could subject regulated parties to a confusing bramble of potentially inconsistent and burdensome rules and regulations. It is critical "to ensure uniformity

---

[20] *See* Federal Acquisition Supply Chain Security Act of 2018, S. 3085, 115th Congress (2018); *see also* Press Release, Senator James Lankford and Senator Claire McCaskill, Senators Lankford and McCaskill Introduce Bipartisan Bill to Safeguard National Security from Supply Chain Security Threats, https://www.lankford.senate.gov/news/press-releases/senators-lankford-and-mccaskill-introduce-bipartisan-bill-to-safeguard-national-security-from-supply-chain-security-threats (June 19, 2018).

[21] *See* CCA Comments at 20–22; Comments of CTIA, WC Docket No. 18-89, at 15–16 (filed June 1, 2018) ("CTIA Comments"); Comments of NCTA – The Internet & Television Ass'n, WC Docket No. 18-89, at 5–9 (filed June 1, 2018) ("NCTA Comments"); NTCA Comments at 11–15; Comments of Rural Broadband Alliance, WC Docket No. 18-89, at 5 (filed June 1, 2018) ("Rural Broadband Alliance Comments"); TIA Comments at 32; USTelecom Comments at 10–12.

(Cont'd on next page)

across the federal government and prevent confusion among industry stakeholders."[22] Inconsistency in the applicable rules for regulated entities would be disastrous. Such a regulatory environment not only would create immense compliance problems for carriers, suppliers, and other entities, but also would have drastic negative effects on markets. As TIA explains, "allowing different agencies to deliver mixed messages regarding the viability of using equipment from a particular supplier on national security grounds could be highly damaging to consumer confidence, to the government, and to the standing of other ICT companies in the global marketplace."[23] As it stands, however, the FCC's proposed rule is "inconsistent with emerging approaches under consideration by Congress."[24] The danger of mismatched rules and restrictions is multiplied when other agencies are involved and may increase the potential harm to consumers and small businesses alike. For these reasons, the FCC should defer to other agencies already actively involved in these issues.

There is no need for the FCC to test the outer limits of its legal authority where Congress and other agencies are actively addressing these supply chain issues and the FCC's own expert consulting group is examining ways to combat cybersecurity risks.[25] CCA argued in its initial comments that the proposed rule violates the Administrative Procedure Act ("APA"), the Communications Act, and the Constitution. Other commenters agree, stating that, for example, "the Commission's authority over cybersecurity is at best dubious, if not altogether spurious."[26]

---

[22] Comments of Motorola Sols., Inc., WC Docket No. 18-89, at 4 (filed June 1, 2018) ("Motorola Comments").

[23] TIA Comments at 60; *see also id.* at 54 (noting risk that there could be "an inconsistent patchwork of restrictions by different agencies across the government").

[24] *Id.* at 48.

[25] *See* CCA Comments at 15–44; *see also infra* 19–23.

[26] ITTA Comments at 2.

The FCC should, in particular, await DHS's assessment of the telecommunications supply chain and allow DHS adequate time to craft a comprehensive and holistic approach to supply chain security grounded in the principles of risk management.

In the alternative, and at a minimum, the record confirms that the FCC should not issue a final rule without requesting further comment on a more detailed proposal. A failure to seek comment on a more detailed proposal would violate the APA both because the existing proposal does not "describe the range of alternatives being considered with reasonable specificity"[27] and because the FCC will have based its decision on outdated information that does not fully consider the overall regulatory environment nor the unintended consequences of FCC action.[28] The FCC should not rush to publish a half-baked final rule when Congress and other expert agencies are actively examining potential actions to address global supply chain security. Rather, the FCC should coordinate with and assist DHS and DoC in a serious review of possible mitigating actions to support national security goals, including ways to offset the cost of potential rip-and-replace measures.

---

[27] *Small Refiner Lead Phase-Down Task Force v. EPA*, 705 F.2d 506, 549 (D.C. Cir. 1983).

[28] *See, e.g.*, *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (a rule is arbitrary and capricious if the agency "failed to consider an important aspect of the problem").

(Cont'd on next page)

III. The Proposed Rule Will Impede Universal Service and Will Not Materially Improve Cybersecurity.

Many comments submitted in response to the NPRM urge the FCC to conduct a fair and rigorous cost-benefit analysis.[29] Although supply chain security is vitally important, the proposed rule's benefits will not outweigh its substantial costs.[30]

A. The Proposed Rule Could Create Immense Costs for Rural Networks.

Neither the FCC nor the proposed rule's supporters have enumerated any of the costs, much less the multiplier in costs that will result from downstream effects. This deficiency is enough to warrant at least a further NPRM and a closer examination of the effects the proposed rule will have on rural carriers and consumers.

The proposed rule will require many carriers to rip and replace any Huawei and ZTE equipment from their networks to preserve their access to USF funding. As CCA and other commenters have explained, rip-and-replace is the likely outcome because of the inability to service and upgrade equipment from prohibited manufacturers.[31] Rip-and-replace becomes even

---

[29] *See, e.g.*, CCA Comments at 29–30; NCTA Comments at 2, 12, 18; Comments of Sagebrush Cellular, Inc., WC Docket No. 18-89, at 2–5 (filed June 1, 2018) ("Sagebrush Cellular Comments"); TIA Comments at 63–64.

[30] CCA Comments 30–33; *see also id.* Berry Decl. at 5–7; *id.* Beehn Decl. at 2–3; *id.* DiRico Decl. at 2–4; *id.* Groft Decl. at 2–3; *id.* Kilgore Decl. at 2–3; *id.* Woody Decl. at 2–4; Comments of Pine Belt Cellular, Inc., WC Docket No. 18-89, at 5–7 (filed June 1, 2018) ("Pine Belt Cellular Comments").

[31] CCA Comments at 9–10; ITTA Comments at 6; Comments of JAB Wireless, Inc., WC Docket No. 18-89, at 4 (filed June 1, 2018) ("JAB Wireless Comments"); Comments of Mark Twain Commc'ns Co., WC Docket No. 18-89, at 4–5 (filed June 1, 2018) ("Mark Twain Comments"); NTCA Comments at 9, 20–21; Puerto Rico Tel. Co. Comments at 6–7; Rural Broadband Alliance Comments at 6; Comments of WTA – Advocates for Rural Broadband, WC Docket No. 18-89, at 6 (filed June 1, 2018) ("WTA Comments").

(Cont'd on next page)

more likely to be widespread if the FCC treats USF dollars as fungible within a provider's operations because carriers then could not shift USF funds to other qualified projects.[32]

The costs of rip-and-replace are staggering. The record demonstrates that some carriers would have to spend millions of dollars—and in some cases, more than $100 million—on just the ***immediate*** costs of ripping and replacing equipment.[33] Even very small carriers will be on the hook for millions of dollars.[34] Rural carriers that chose "the most cost-effective option" available to them at the time of purchase will be forced to rebuild their networks at a cost substantially greater than they spent to build the networks in the first place.[35] This would be an ironic result indeed during a time when the FCC imposes budget caps and conducts auctions intended to minimize the extent of universal service support, thereby dictating that carriers seek out greater efficiencies in delivering the promise of universal service.

The proposed rule will impose costs in addition to expenditures on new equipment and installation. The record demonstrates that carriers could have to spend more on services and could lose revenue from a variety of sources. For example, reduced coverage areas due to the cost to deploy new equipment and network outages resulting from the installation of that

---

[32] NPRM ¶ 16 (requesting comment on whether the rule should "prohibit the use of any USF funds on any project where equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain is being purchased or obtained"); *see* CCA Comments at 44–45; *cf.* Comments of TracFone Wireless, Inc., WC Docket No. 18-89, at 2–3 (filed June 1, 2018) ("TracFone Comments").

[33] *See* CCA Comments, Beehn Decl. at 2; *id.*, DiRico Decl. at 3; *id.*, Woody Decl. at 2–3.

[34] Pine Belt Cellular Comments at 6–7.

[35] *Id.* at 6; *see also* Mark Twain Comments at 4–5; Rural Broadband Alliance Comments at 2–3; Sagebrush Cellular Comments at 2–3; WTA Comments at 3–5.

(Cont'd on next page)

equipment will cause carriers to forego revenue from roaming contracts.[36] The proposed rule also could cause "price crunches in cases where a carrier seeks to effectuate large deployments or needs to perform equipment upgrades in short order without the benefit of abundant advanced planning, and no longer may purchase from suppliers that commonly have greater inventory volumes readily available."[37]

Uncertainty exacerbates both direct and indirect costs for carriers. Market uncertainty naturally will lead to overall higher prices for equipment and services and borrowing costs will rise. Indeed, the proposed rule would harm recipients of universal service and the consumers they serve by removing cost-effective suppliers from the equipment marketplace. Market competition has promoted the development of new products, services, and technologies, which in turn has engendered greater selection and better pricing in a manner that accrues to the benefit of fixed-budget universal service mechanisms. But, if enacted, this proposal will substantially narrow the scope of products and services available to rural operators. A prohibition on the use of certain suppliers that helped drive competition in equipment pricing runs counter to the cost-efficiency objectives underlying the FCC's use of auctions and caps.[38] Moreover, carriers' investments currently are and will continue to be chilled because of the uncertainty with respect to whether any company will be blacklisted in the future.[39] All told, the costs of compliance with the proposed rule will cause certain rural carriers to significantly reduce their coverage

---

[36] CCA Comments at 10–11; *id.*, Woody Decl. at 2; Pine Belt Cellular Comments at 6–7.

[37] ITTA Comments at 5.

[38] CCA Comments at 6–7; *id.*, Berry Decl. at 3–6; NTCA Comments at 21 & n.33.

[39] CCA Comments at 7, 11–13; ITTA Comments at 6; Mark Twain Comments at 2–3; NTCA Comments at 21; *see also* NCTA Comments at 12 ("Communications service providers need to have a clear understanding regarding the identity of blacklisted vendors and/or blacklisted vendor equipment to avoid uncertainty in buying decisions.").

(Cont'd on next page)

areas and reduce investment in advanced networks—or go out of business altogether, if forced to immediately replace their equipment.[40]

To avoid the costs of immediate rip-and-replace, an affected carrier will have to forego USF support, which is itself a substantial cost.[41] Cost multipliers exist down this route, too, especially if the FCC treats USF funds as fungible—that is, if the FCC bans USF funds from being used on any project that involves equipment or services from a targeted company, even if the USF dollars are not themselves spent on that equipment or those services. In that scenario, carriers would be unable to enter into or perform on roaming agreements with other carriers, resulting in lost revenue and potentially damages for breach of contract. Carriers also could lose the ability to work with Lifeline recipients or other recipients of USF dollars, such as hospitals and schools. All of those costs would come on top of the lost USF support for network equipment and services. The bottom-line result for a carrier that chooses to forego USF dollars rather than comply with the proposed rule is likely to be the same as if the carrier did try to comply: smaller coverage areas, decreased investment in advanced technology, and the possibility of shuttering the business.

B. The Proposed Rule Will Harm Consumers, Small Businesses, and Local Governments.

Consumers will suffer from any decision that undermines investment and operations in rural America. Rural consumers will see a reduction in or be denied the same level of service provided to consumers in the rest of the country, because investment in advanced networks will be significantly reduced and delayed. Ultimately, rural consumers will pay more for less, as the

---

[40] CCA Comments, Beehn Decl. at 2–3; *id.* DiRico Decl. at 2–4; *id.* Groft Decl. at 2–3; *id.* Kilgore Decl. at 2–3; *id.* Woody Decl. at 2–4.

[41] *See, e.g.*, CCA Comments, Woody Decl. at 1–2.

(Cont'd on next page)

proposed rule's costs trickle down into the bills paid by end-users.[42] Many of those rural customers are local governments, which will be dramatically affected. Individual consumers thus will see diminished municipal services in addition to their telecommunications and information services.

Private networks' ability to place calls for emergency services also will be threatened. Advancing claimed national security and foreign policy goals means little if Americans cannot contact emergency services because of coverage-area reductions or interruptions in service.[43] To be sure, Motorola points out that the DoC has barred Huawei equipment from the First Responder Network Authority's National Public Safety Broadband Network ("NPSBN").[44] But the NPSBN goes above and beyond the simple ability for individuals to contact emergency services. Rather, the NPSBN is a nationwide dedicated public safety network, and the considerations are therefore very different.

The record reflects that other USF recipients could be adversely affected. E-Rate recipients, such as schools and libraries,[45] will see their costs rise. The Lifeline program also could be severely impacted, especially if the FCC prohibits the use of USF funds on programs that utilize any equipment or services provided by targeted companies.[46] Even if the FCC does not go in that direction, consumers who benefit from the Lifeline program would still be among the hardest hit, because they are the least able to withstand price increases and among the most

---

42 CCA Comments at 7, 13–14; NTCA Comments at 20–21.

43 *See* CCA Comments at 8, 31; NTCA Comments at 2; Sagebrush Cellular Comments at 3–4.

44 *See* Motorola Comments at 5–6.

45 *See* Comments of the Am. Library Ass'n, WC Docket No. 18-89 (filed June 1, 2018) ("ALA Comments"); Comments of State E-Rate Coordinators Alliance, WC Docket No. 18-89 (filed May 29, 2018).

46 TracFone Comments at 2–3.

vulnerable to the day-to-day harms caused by reductions in coverage and service quality. The proposed rule thus could impact the stakeholders least able to absorb the costs of the FCC's supply chain priorities.

Finally, the FCC's Regulatory Flexibility Analysis, and its treatment of small businesses overall, is inadequate. Small businesses will be the most adversely affected by the proposed rule.[47] The FCC must account for the fact that the proposed rule's immense costs will fall mostly on those entities least capable of shouldering them.

C. Any Benefits from the Proposed Rule Are Substantially Outweighed by the Costs.

The Associations fully recognize the seriousness of threats to network security and are committed to addressing them. But the Associations cannot support the approach taken by the proposed rule, as the costs vastly outweigh any possible benefits.

Indeed, the record reflects that no one is able to elucidate the proposed rule's benefits in any meaningful way. The 2012 House Permanent Select Committee on Intelligence report on which the FCC relies is devoid of detail, and the FCC has not supplemented that report with anything of substance. Nor have any commenters identified real benefits. The benefits that commenters hypothesize could flow from the proposed rule, such as improved market confidence, decreased costs from proactive cybersecurity protection, and reduced losses from cyber breaches, are speculative.[48] These benefits depend on believing that the proposed rule eliminates a serious risk to cybersecurity, but that risk is amorphous and ill-defined.[49] And it is

---

47 *See* CCA Comments at 32; NTCA Comments at 18–21, 23–24.

48 *See* TIA Comments at 66–70.

49 *See, e.g.*, *id.*at 36 (describing the "*possible* threat vectors" that the proposed rule "*seems* most targeted at addressing") (emphases added).

(Cont'd on next page)

highly unlikely that costs from "malicious cyber activity" or proactive cybersecurity efforts would decrease on account of the proposed rule.[50] It is unrealistic to believe that governments, carriers, and consumers will reduce reliance on proactive cybersecurity efforts, such as up-to-date scanning software and internal and external audits, if the proposed rule is implemented. Nor is it reasonable to expect malicious hacking and other costly breaches to decrease in frequency and magnitude in coming years because of the FCC's proposed action in this proceeding. All of these supposed benefits, moreover, are concededly dependent on concerted interagency or even worldwide action.[51]

Prohibiting the use of USF funds to purchase Huawei and ZTE equipment will not materially lessen the vulnerability of America's vast telecommunications networks. The amount of targeted companies' equipment in USF-supported networks represents a relatively small share of America's networks overall.[52] If anything, the proposed rule will only increase problems associated with "white labeling," which is the practice of selling a company's products under a different brand name.[53]

Network infiltration, moreover, can "be facilitated by equipment or services ***interfacing*** with the network," and "USF-funded networks are interconnected with the rest of the vast [American] communications infrastructure."[54] Huawei and ZTE sell equipment and services to

---

[50] *Id.* at 69.

[51] *See, e.g.*, *id.* at 84 ("[N]o single country can address the threats from potentially malicious actors or high-risk suppliers by itself.").

[52] *See* CCIA Comments at 3 ("[T]he U.S. market share of Huawei and ZTE are relatively small compared to the rest of the world.").

[53] Rural Broadband Alliance Comments at 8.

[54] ITTA Comments at 4–5 (emphasis added); TIA Comments at 7.

(Cont'd on next page)

many carriers; they do not confine their sales to USF recipients. And even if all Huawei and ZTE equipment and services were excised from the United States, risk would still exist because American networks and devices would still interface with foreign networks that include equipment and services provided by targeted companies.[55] The proposed rule simply will not accomplish its stated goals.

IV. The Proposed Rule Discriminates Against Smaller, Rural Carriers and Is Not Tailored to the Scope of the Asserted Risk.

The proposed rule will yield few benefits in part because it only prevents the use of targeted equipment by USF recipients, not other companies. The proposed rule is thus arbitrary and capricious because it discriminates against predominantly small, rural carriers without fully addressing the asserted problem.[56]

Any risk posed by Huawei and ZTE is not confined to USF recipients. TIA noted that "[i]t is logical that if equipment or services from certain companies is deemed to pose a sufficient threat to require action in the USF context, such equipment or services would also pose a similar threat in other contexts as well."[57] USF-supported networks are just "a small factor" in the larger cybersecurity ecosystem.[58] Thus, regulations will only "effectively protect the communications supply chains" if they "apply to all U.S. telecom and information network operators."[59]

---

55 *See* NTCA Comments at 16.

56 *See* CCA Comments at 35; *Motor Vehicle Mfrs. Ass'n*, 463 U.S. 29, 43 (1983); *Home Box Office, Inc. v. FCC*, 567 F.2d 9, 36 (D.C. Cir. 1977).

57 TIA Comments at 19.

58 *Id.* at 67.

59 AT&T Comments at 3.

(Cont'd on next page)

It would be unfair and unworkable for the FCC to adopt a regime that prescribes the equipment and services carriers may and may not use, based solely on whether the carrier receives USF support. In this regard, commenters on the NPRM are united in recognizing the need for consistency; "[r]estrictions should be consistent across the government to the greatest extent possible" to prevent a "compliance nightmare."[60] Inconsistent regulatory burdens would unfairly skew the market. As AT&T explains, "providers' choices of equipment and services strongly impact[s] both cost and innovation." If the FCC "restrict[s] the equipment and service choices of some market participants but not others, as would result from limiting such measures to USF recipients, [it] would potentially distort competition and harm consumers."[61] Ultimately, "in today's highly competitive environment, restrictions and regulations that apply only to a subset of the industry threaten to do more harm than good."[62]

V. The Proposed Rule Violates the Communications Act and the Constitution.

Section 254 of the Communications Act does not give the FCC authority to condition receipt of USF dollars on national security concerns.[63] None of the Section 254(b) principles supports the proposed rule, as CCA demonstrated in its opening comments.[64] The FCC cannot treat "national security" as a universal service principle. To begin, Congress directed that new universal service principles adopted pursuant to Section 254(b)(7) must be approved by ***both***

---

60 TIA Comments at 47.

61 AT&T Comments at 3.

62 *Id.* at 4.

63 47 U.S.C. § 254. Section 254's specificity trumps Section 201's general grant of authority. *See Gozlon-Peretz v. United States*, 498 U.S. 395, 407 (1991); CCA Comments at 16.

64 CCA Comments at 16–19.

(Cont'd on next page)

"the Joint Board ***and*** the Commission."[65] Substantively, Congress prescribed that new universal service principles must be "necessary and appropriate for the protection of the public interest, convenience, and necessity and . . . consistent with" the rest of the Communications Act.[66] It is a longstanding interpretive principle that broad terms such as the "public interest" must be read in reference to the specific regulatory goals at hand; in using that term, Congress did not intend to bestow unfettered authority on the FCC.[67] Nothing in Section 254 suggests that national security is a universal service concern. Rather, Congress made it clear that in the context of universal service, the public interest means expanded access to quality telecommunications and information services and a regulatory environment that is equitable, nondiscriminatory, and predictable.[68] National security is dissimilar to any of the principles enumerated in Section 254(b).[69] If Congress expected the FCC to consider national security or to incorporate another agency's national security-related determination, it would have said so.[70] And even if the "public interest" could be read to include national security in this context, it is neither

---

[65] 47 U.S.C. § 254(b)(7) (emphasis added); CCA Comments at 20. TIA misunderstands the Section 254(b) framework and erroneously suggests that the FCC has authority to adopt the proposed rule because furthering national security is in the public interest. TIA Comments at 24. That is incorrect. At the very least, the FCC must adopt national security as an express universal service principle after the Joint Board has recommended it do so.

[66] 47 U.S.C. § 254(b)(7).

[67] *See Nat'l Broad. Co. v. United States*, 319 U.S. 190, 216 (1943).

[68] *See* 47 U.S.C. § 254(b).

[69] CCA Comments at 26.

[70] *See, e.g.*, 47 U.S.C. § 305(c) (authorizing President to allow foreign governments to operate radio stations in certain locations and under certain conditions if doing so is "consistent with and in the interest of national security"); *id.* § 1404(a), (c) (prohibiting payments to any "person who has been, for reasons of national security, barred by any agency of the Federal Government from bidding on a contract, participating in an auction, or receiving a grant").

(Cont'd on next page)

"necessary" nor "appropriate" to adopt national security as a universal service principle because other agencies are better suited for this type of regulation.[71]

Similarly, the FCC cannot re-define "universal service" under Section 254(c)(1) on the ground that the proposed rule is in "the public interest."[72] Again, the FCC first has to seek the Joint Board's recommendation. Congress directed in Section 254(c)(1) that the Joint Board "recommend[s]," and the FCC "establish[es], the definition of the services that are supported by Federal universal service support mechanisms."[73] Even if the FCC followed the appropriate procedure for re-defining "universal service," that term refers to telecommunications ***services***, not ***vendors*** who provide the equipment and services that enable carriers to offer telecommunications services. Nothing about the concept of universal service suggests that Congress anticipated such an inversion of the definition of "universal service" as the FCC suggests in the NPRM.[74]

Nothing else in the Communications Act could plausibly grant the FCC legal authority to promulgate the proposed rule. In passing, the FCC's NPRM cites 47 U.S.C. § 1004.[75] That provision requires that carriers "ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations

---

71 CCA Comments at 20–23.

72 47 U.S.C. § 254(c)(1).

73 CCA Comments at 27.

74 *Id.*; *see also* TIA Comments at 24 (agreeing that the proposed rule is not "equivalent to establishing a new definition" of universal service).

75 NPRM ¶ 36 n.64.

(Cont'd on next page)

prescribed by the Commission."[76] Section 1004 is both too narrow and too broad to justify the proposed rule. It is too narrow because it is focused merely on switching premises and it is too broad because it is not limited to the USF.

The FCC's oblique reference to Section 151's invocation of "the national defense" also is unavailing.[77] Specifically, Section 151 tasks the FCC with

> regulating interstate and foreign commerce in communication . . . to make available, so far as possible, to all the people of the United States, . . . a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense, for the purpose of promoting safety of life and property . . . , and for the purpose of securing a more effective execution of this policy by centralizing authority . . . .[78]

Section 151's emphasis on the expansion of access to telecommunications networks at reasonable prices ***undermines*** the proposed rule.[79] In fact, the policies Congress built into the Communications Act and the 1996 Telecommunications Act counsel strongly against the proposed rule.[80] Even if Section 151's general policy statement supported the proposed rule, it must yield to the more specific instructions Congress enumerated in Section 254(b).[81]

The proposed rule also raises very serious constitutional questions. Communications providers relied on the legality of the equipment they purchased. For example, one CCA member submitted a comment in which it describes relying on specific representations from

---

[76] 47 U.S.C. § 1004.

[77] NPRM ¶ 36 n.63.

[78] 47 U.S.C. § 151.

[79] *See* CCA Comments at 4, 27, 36.

[80] *See id.* at 27–28; *see also* 47 U.S.C. § 256(a)(1) (directing the FCC "to promote nondiscriminatory accessibility by the broadest number of users and vendors of communications products and services to public telecommunications networks used to provide telecommunications service").

[81] *See supra* note 63.

(Cont'd on next page)

government officials.[82] Other providers report similar experiences. The proposed rule, furthermore, calls into question the ongoing validity of existing contracts. And existing equipment cannot be maintained without services that need to be provided by the equipment vendor. All of this will happen through a regulation targeted at a specific class (USF recipients who are customers of a set of certain companies) without giving them the opportunity to review and rebut the evidence supporting the rule.

Under these circumstances, the proposed rule violates multiple clauses of the Fifth Amendment to the United States Constitution. Depriving carriers of the use of their equipment is an unconstitutional taking.[83] Demolishing carriers' investment-backed reliance interests violates Due Process.[84] Carriers' due process rights are further infringed because they have not been given the opportunity to review and rebut evidence providing the basis for what amounts to a confiscation of their property.[85] These substantial deficiencies weigh in favor of withdrawing the proposed rule or, at the very least, considering measures that may mitigate the proposed rule's harmful effects as part of a Further Notice of Proposed Rulemaking.

VI. If the FCC Nonetheless Moves Forward, It Should Adopt Provisions to Mitigate the Proposed Rule's Harmful Impact.

If the FCC moves forward with this rulemaking, it should adopt provisions that mitigate the immense costs the proposed rule will otherwise engender. Three mitigation measures are particularly important: (1) an extended compliance period; (2) robust grandfathering rules; and

---

[82] Sagebrush Cellular Comments at 2.

[83] *See Lucas v. S.C. Coastal Council*, 505 U.S. 1003, 1015 (1992); *Penn Cent. Transp. Co. v. City of New York*, 438 U.S. 104, 127 (1978); *see also* CCA Comments at 42–44.

[84] *See Gen. Motors Corp. v. Romein*, 503 U.S. 181, 191 (1992); *see also* CCA Comments at 41.

[85] *See Ralls Corp. v. Comm. on Foreign Inv. in the U.S.*, 758 F.3d 296, 319 (D.C. Cir. 2014); *see also* CCA Comments at 41–42.

(3) adequate transitional funding for adversely affected carriers. It is likewise important for the FCC to (4) make crystal clear that the scope of the rule does not prevent spending USF funds on projects that currently utilize or depend on equipment, services, or devices manufactured or provided by targeted companies; (5) limit the rule to particular types of equipment; (6) not automatically cover parents, subsidiaries, or affiliates; and (7) provide for waivers.

1. Compliance Period. It will take 10 years or more for carriers to entirely rip and replace Huawei and ZTE equipment from their networks.[86] Thus, the FCC should not require full compliance until at least 10 years after adoption of a final rule. It is important that "existing equipment [is] rolled off in an orderly fashion"; if "entire networks [are] torn out prematurely," the results would be "potentially catastrophic."[87] Alternatively, the FCC could adopt a phase-in approach with a lengthy period of time for full compliance.[88] Shorter compliance timeframes also should be accompanied by reimbursement or offset funding for providers above and beyond the funding discussed below.

2. Grandfathering Rules. To allow for a smooth transition and to lessen the disruption to the development of advanced 4G VoLTE and 5G networks, the FCC should include

---

[86] *See* CCA Comments at 45; Sagebrush Cellular Comments at 6–7 (10 years required to plan, rip, and replace network equipment); NTCA Comments at 23–24 ("[S]mall 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."); Rural Broadband Alliance Comments, Domain5 Report at 3 ("It will take small, remote and rural wireless providers at least five years to replace the hardware and software, to obtain professional support services, and retrain the technical staff needed to operate and maintain the new equipment."); *see also* NCTA Comments at 16 ("Given the long lead time associated with procuring communications network equipment, the Commission should provide for an interim transition period to adjust to any new supply constraints engendered by the rules.").

[87] Rural Broadband Alliance Comments at 14.

[88] CCA Comments at 45; US Telecom Comments at 15.

(Cont'd on next page)

robust grandfathering provisions. As discussed in CCA's initial comments, the FCC should grandfather existing contracts, including multiyear contracts and contracts for future upgrades and/or services. It is also critical that the FCC grandfather existing equipment and the upgrades or services needed to support that equipment for its normal useful life.[89] As NTCA notes, "software updates also should be explicitly allowed."[90] Existing consumer devices should also be grandfathered to ensure that end-users do not experience interruptions in their services or new vulnerabilities resulting from an inability to download software updates.[91]

3. Transitional Funding. Many rural carriers will be drastically harmed by the proposed rule and some will go out of business altogether.[92] Additional funding would be vitally important to assist carriers in weathering the immense costs of ripping and replacing their network equipment.[93] Because of existing constraints on the USF budget, money may need to be appropriated by Congress.[94] This is another reason that, as discussed above, the FCC should defer action at this time and allow Congress to take the lead on supply chain security.

---

89 ALA Comments at 3; CCA Comments at 46–47; NCTA Comments at 15–16; NTCA Comments at 24; Puerto Rico Tel. Co. Comments at 7; WTA Comments at 6.

90 NTCA Comments at 24.

91 TracFone Comments at 6.

92 *See supra* 11–14.

93 *See* CCA Comments at 45; NTCA Comments at 24; Rural Broadband Alliance Comments at 14; JAB Wireless Comments at 7.

94 *See Connect America Fund; A National Broadband Plan for Our Future; Establishing Just and Reasonable Rates for Local Exchange Carriers; High-Cost Universal Service Support; Developing an Unified Intercarrier Compensation Regime; Federal-State Joint Board on Universal Service; Lifeline and Link-Up; Universal Service Reform – Mobility Fund*, WC Docket No. 10-90, GN Docket No. 09-51, WC Docket No. 07-135, WC Docket No. 05-337, CC Docket No. 01-92, CC Docket No. 96-45, WC Docket No. 03-109, WT Docket No. 10-208, Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd 17672, ¶ 18 (2011) (*USF/ICC Transformation Order*) (announcing budget cap mechanism for high-cost USF program).

(Cont'd on next page)

4. Direct Expenditure of USF Funds. If the FCC extends the proposed rule to cover any USF-funded project or service that utilizes or depends on equipment, services, or devices manufactured or provided by targeted companies, it will increase the burden on carriers and recipients of USF programs other than high-cost support, such as Lifeline.[95] For that reason, the FCC should make it clear that the rule covers only direct expenditures of USF funds.

5. Applicability to Certain Equipment Only. The Associations encourage the FCC to prohibit only specific equipment for which there is identifiable evidence that the security risks present cannot be fixed through software patching or other mechanisms.[96] The Associations also agree with TIA that restricting services will "create problems in scenarios where non-prohibited [information and communications technology] companies may need to temporarily operate prohibited equipment during a transition period."[97] The FCC thus should not prohibit services provided by targeted companies at least during the transition period, and the Associations urge the FCC to not prohibit ***any*** services, so long as they are provided by an American subsidiary or affiliate of a targeted company, because services pose an inherently lower risk than equipment manufactured overseas.

6. Treat Parents, Subsidiaries, Affiliates, and Joint Ventures Separately. There is no reason to believe that subsidiaries, affiliates, or joint ventures necessarily present the same security risks as a related company, and the FCC should not treat related companies the same

---

95 *See* CCA Comments at 44–45; Tracfone Comments at 2–3.

96 *See* CCA Comments at 44.

97 TIA Comments at 53.

(Cont'd on next page)

without a specific reason for doing so. That is especially true where an American subsidiary or affiliate provides only servicing, as noted immediately above.[98]

7. Waivers. The FCC should make waivers[99] available to USF recipients that meet the "good cause" standard provided in 47 C.F.R. § 1.3.[100]

These mitigating measures can take numerous forms and combinations. Although some commenters have provided feedback on the types of mitigating measures the FCC should adopt if it proceeds with this rulemaking, stakeholders are unable to comment on a specific combination or set of alternative combinations of mitigation provisions because the FCC has provided none. The FCC, in fact, has failed to provide any specific proposals on acceptable mitigation efforts. To promulgate a final rule without first seeking additional comment on a more specific proposal would be arbitrary and capricious.[101] It is important for stakeholders to further comment on a rule that includes mitigation measures if they are to participate

---

[98] *See* CCA Comments at 44. TIA provides no evidence or reasons for supporting an automatic extension of a blacklisting to parents, subsidiaries, or affiliates, and its suggested exclusion for joint ventures is arbitrary. *See* TIA Comments 57. The better approach is to treat parents, subsidiaries, affiliates, and joint ventures as individual entities, absent evidence for treating them as alter egos of targeted companies.

[99] Letter from Senators Rubio, Van Hollen, and Cotton to Wilbur Ross, Secretary, Dept. of Commerce (June 25, 2018) (urging DoC "to immediately provide assurances, in the form of guidance and waivers, to both telecommunications operators and other customers who wish to remove ZTE software, hardware, and technology . . . from their network infrastructure and install products from other suppliers in the market, as well as to suppliers who are in compliance with U.S. export controls and seek to provide these customers with alternative products to ZTE items."), *available at* https://goo.gl/SSMPpS.

[100] *See Vt. Pub. Serv. Bd. v. FCC*, 661 F.3d 54, 65 (D.C. Cir. 2011) (noting that a waiver "process is a 'sign of reasonableness,'" and "an effort by an agency 'to cabin'" the regulation's "'potential sweep'" (quoting *Nat. Res. Def. Council v. EPA*, 822 F.2d 104, 120 (D.C. Cir. 1987)); *Rural Cellular Ass'n v. FCC*, 588 F.3d 1095, 1104–05 (D.C. Cir. 2009) (assessing rule's fairness by looking to whether regulated parties had a meaningful opportunity "to obtain an exception"); *see also* CCA Comments at 46; JAB Wireless Comments at 8.

[101] *See* CCA Comments at 47–48.

meaningfully in this rulemaking. The FCC also should not move forward without a more detailed and explicit economic analysis that quantifies the benefits for comparison against the costs and factors in any mitigation measures. The current rulemaking does not adequately address costs and benefits.

VII. Conclusion.

The FCC is right to be concerned about the security of the telecommunications supply chain. The record developed in this rulemaking, however, confirms the Associations' initial comments: the proposed rule is neither a permissible nor effective means of furthering national security. The FCC should defer to Congress and other expert agencies and withdraw the proposed rule. At the very least, the FCC should seek further comment on a revised proposed rule that incorporates provisions designed to mitigate the immense harms that will otherwise be imposed on rural carriers and consumers.

Respectfully submitted,

/s/ Matt Schruers
Matt Schruers
John A. Howes, Jr.
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION
655 15th Street, NW, Suite 410
Washington, DC 20005
(202) 783-0070
www.ccianet.org

/s/ Genevieve Morelli
Genevieve Morelli
Michael J. Jacobs
ITTA – THE VOICE OF AMERICA'S BROADBAND PROVIDERS
1101 Vermont Avenue, NW, Suite 501
Washington, DC 20005
(202) 898-1520
www.itta.us

/s/ Michael R. Romano
Michael R. Romano
NTCA—The Rural Broadband Association
4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
(703) 351-2016
www.ntca.org

/s/ Rebecca Murphy Thompson
Steven K. Berry
Rebecca Murphy Thompson
Courtney Neville
COMPETITIVE CARRIERS ASSOCIATION
601 New Jersey Avenue, NW, Suite 820
Washington, DC 20001
(202) 449-9866
www.ccamobile.org

Theodore B. Olson
Thomas H. Dupree Jr.
Andrew G.I. Kilberg
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, NW
Washington, DC 20036
(202) 955-8500
www.gibsondunn.com

July 2, 2018