Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 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 HUAWEI TECHNOLOGIES CO., LTD AND HUAWEI TECHNOLOGIES USA, INC.

Glen D. Nager
Bruce A. Olcott
Ryan J. Watson
Vivek Suri
Parker Rider-Longmaid

JONES DAY
51 Louisiana Ave, NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)

Andrew D. Lipman
Russell M. Blau
David B. Salmons
Catherine Kuersten
Patricia Cave

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave, NW
Washington, DC 20004
(202) 739-3000
(202) 739-3001 (Fax)

Counsel to Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc.

Date: July 2, 2018

SUMMARY

The comments submitted in response to the NPRM confirm, as Huawei stated in its opening Comments, that the Commission's proposed rule is both legally and factually unsupported. Those parties encouraging the Commission to blacklist a handful of companies from supplying equipment or services to USF support recipients are largely those companies' competitors, who would directly benefit from such a rule. The extensive costs of the blacklist, by contrast, would be borne by carriers and institutions that receive USF support, a number of whom rely on equipment manufactured by Huawei, by their customers, and by the U.S. economy as a whole.

The U.S. cannot afford to become the only country in the world that lacks access to the best communication technologies. Huawei is a global leader in key segments of the telecommunications equipment market, particularly (but not exclusively) for mobile networks, with leading positions in LTE systems, Radio Access Networks, and Mobile Packet Core. Huawei has played a key role in development of 5G standards and has been an innovation leader in 5G deployment. Worldwide, it has deployed by far the largest share of broadband access equipment (FTTx, DSl, and CMTS/CCAP). But its presence in the U.S. market has been artificially restricted by unfounded allegations and suspicions based solely on misperceptions about Huawei's relationship with the government of China. As Huawei showed in its initial Comments, the reality is that it is an independent, privately-owned business that is no more subject to the control of the Chinese Government than American companies are controlled by the U.S. Government. Huawei's products are sold in the U.S. by its Texas-based subsidiary, which is an American corporation governed by American law.

American consumers are already paying a high cost in lost opportunities and reduced competition due to the *de facto* exclusion of Huawei from many network procurements; these effects

would be magnified by a *de jure* prohibition on use of USF funds. Where Huawei is allowed to bid, its presence restrains the pricing of other vendors, and consumers benefit regardless of who wins the bid. Because Huawei is often not allowed to bid in U.S. procurements, average prices for network equipment are higher here than in most other countries; and U.S. customers generally pay higher prices for a lower level of mobile service than consumers elsewhere. Allowing Huawei to compete freely could yield savings of at least $20 billion in building U.S. mobile infrastructure between 2017 and 2020, which would likely be passed through to consumers. Conversely, restrictions on Huawei will result in excessive profits for a handful of other equipment suppliers in this highly concentrated market, which will give those companies an incentive to transfer their U.S. profits to improve their positions in other countries where they face more vigorous competition. This will lead to a vicious cycle in which investment and innovation is driven into non-U.S. markets and consumers in this country will fall farther and farther behind the rest of the world.

Furthermore, banning existing users of Huawei equipment from obtaining replacement parts or services, or adding to their networks, would impose disproportionate costs on them in the hundreds of millions of dollars. There are serious problems with a "mix-and-match" network approach, so many of these carriers would have to retire existing equipment long before the end of its useful life, at huge expense. Some rural carriers indicate they would likely forfeit USF support, and be forced to scale back their network coverage, rather than rip out and replace their core network.

These high costs, which would particularly harm Americans in remote and low-income areas, cannot be justified by the supposed national security benefits of the proposed rule, because these are speculative. At best, the proposed rule would only target one of many potential threats to

the integrity of the supply chain – that is, hypothetical threats from products deliberately compromised by their manufacturer – leaving many other vulnerabilities unaddressed. But even that theoretical benefit is unlikely to be achieved, because the vague criteria for identifying national security threats are unlikely to be accurate. Despite the obvious desire of the supporters of this rulemaking to target Huawei in particular, there has never been any evidence of any actual harm or even potential harm to the network from the use of Huawei equipment. The governments of many countries, including the United Kingdom, Canada, and Finland, have expressed their confidence in Huawei's equipment. And the U.S. Government has never notified Huawei customers of even a single hidden flaw in any Huawei product. Eliminating Huawei's products from U.S. networks would have no benefit, because these products are not a source of any harm to begin with.

Beyond this, the initial comments confirm Huawei's view that the proposed rule exceeds the Commission's statutory authority. Most commenters agree that the FCC's authority over the Universal Service Fund does not encompass national-security concerns, and interjecting such concerns into the funding process would violate the statutory universal service principles. Further, it would contravene the established principle that any conditions attached to Federal funds must be clearly expressed in the governing statute, not read in by interpretation. And, even if the FCC did have authority to impose national-security conditions on USF recipients, it would have to make the relevant determinations itself (which virtually every commenter agrees it lacks the resources and expertise to do), not co-opt those made by other elements of the Government.

In addition, even if the FCC did have statutory authority here, the way it proposes to exercise that authority in the NPRM would be arbitrary and capricious. The comments confirm Huawei's view that the proposed rule is unduly vague and offers no meaningful guidance to affected parties. The proposal irrationally targets specific named sellers of equipment and services

rather than particular products, and therefore draws lines that bear no relationship to the supposed threat. Further, this focus on specific vendors irrationally ignores the fact that nearly every seller of telecommunications equipment has a substantial presence in China (including, in some cases, joint ventures with State-owned enterprises) and relies on Chinese-manufactured components. If the perceived threat emanates from the Chinese Government's supposed ability to penetrate China-based manufacturing operations, then just banning one or two companies will not be sufficient; the Commission would have to ban purchase of virtually all network equipment, which is of course absurd. Instead, the Commission should focus on risk-based approaches such as the NIST Cyber-security Framework and the CSRIC recommendations; but the NPRM irrationally fails even to consider such alternatives.

Finally, the comments confirm that the proposed rule violates targeted companies' procedural rights. Huawei has explained that due process requires giving a targeted company notice, the opportunity for a meaningful individualized hearing, and the opportunity to review and respond to the evidence against it before the company may be blacklisted. No commenter denied this point; quite the contrary, one of the proposed rule's most vocal supporters explicitly agrees that the Commission should afford due process to targeted companies.

For these and other reasons detailed in the body of the Reply Comments, the Commission should reject the proposed rule.

Table of Contents

I. INTRODUCTION 1

II. THE COMMENTS PROVIDE NO SUPPORT FOR THE FCC'S CLAIMED LEGAL AUTHORITY 3

A. Other Commenters Agree, and Clear-Statement Principles Confirm, that the FCC Lacks Statutory Authority to Treat National-Security Concerns As Dispositive In the USF Context 4

1. Many commenters agree that the Commission lacks the statutory authority to treat national-security concerns as dispositive in making USF decisions 4

2. The Commission lacks authority to impose the proposed restrictions under the clear-statement principles governing offers of Federal money 5

B. TIA's Arguments Do Not Support The FCC's Claimed Authority 10

1. The statutory provisions invoked by TIA do not support the proposed rule. 11

2. The Tenth Circuit's decision upholding the FCC's authority to impose broadband-related conditions on USF funding does not support the proposed rule. 12

3. TIA cannot cure the Commission's lack of authority by co-opting other government actors' national-security determinations. 15

C. The Other Comments Supporting The Proposed Rule Confirm The Commission's Lack Of Statutory Authority 16

III. THE PROPOSED RULE IS ARBITRARY AND CAPRICIOUS 18

A. The Comments Confirm That the Proposed Rule Is Unduly Vague and Offers No Meaningful Guidance to Affected Parties 18

B. The Comments Confirm that the Proposed Rule Draws Irrational Lines 19

C. The Comments Confirm that the Proposed Rule Reflects Irrational Decisionmaking 23

IV. THE COMMENTS CONFIRM THAT THE COSTS OF THE PROPOSED RULE WOULD VASTLY OUTWEIGH ANY POTENTIAL BENEFITS 29

A. The Proposed Rule Would Impair Competition, Discourage Innovation, and Harm the U.S. Economy 32

1. The proposed rule would reduce competition and cost the American economy billions of dollars 32

2. The proposed rule would deny Americans access to Huawei's market-leading technology 34
B. The Proposed Rule Would Impose Substantial Costs on Rural Carriers and Other USF Recipients by Restricting Servicing or Upgrades of Existing Equipment, and Imposing Burdensome Compliance Obligations 39
1. The proposed rule would result in higher prices for rural carriers due to reduced competition 39
2. The proposed rule will strand investment by precluding carriers from servicing or upgrading existing equipment 43
3. The proposed rule would undermine the goal of universal service 47
C. TIA's Arguments That Costs Would Be Limited Are Unfounded 48
1. Cost of U.S. Government intervention in the marketplace 48
2. Harm to competition 50
D. The Comments Confirm That Benefits Would Be Speculative and Minimal 53
E. TIA's Analysis of Benefits is Logically Flawed and Factually Unfounded 54
1. Quality of service 54
2. Reduction of costs for cyberattacks and breaches 55
3. Consumer Confidence 56
V. EVEN IF THE COMMISSION HAD AUTHORITY TO EXCLUDE A COMPANY FROM SELLING EQUIPMENT, IT COULD NOT DO SO WITHOUT FIRST PROVIDING NOTICE AND A MEANINGFUL HEARING 57
VI. THE PROPOSED RULE RELIES ON UNSUPPORTABLE FACTUAL ALLEGATIONS AGAINST HUAWEI 61
VII. THE COMMENTS SUPPORTING THE PROPOSED RULE ARE OTHERWISE UNPERSUASIVE 65
VIII. CONCLUSION 68

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 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 HUAWEI TECHNOLOGIES CO., LTD
AND
HUAWEI TECHNOLOGIES USA, INC.

Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc. (collectively, "Huawei"), by their undersigned counsel, submit these reply comments in response to comments recently filed relating to the Federal Communications Commission ("FCC" or "Commission") Notice of Proposed Rulemaking ("NPRM") released in this docket (FCC 18-42) on April 18, 2018, and published in the Federal Register on May 2, 2018 (83 Fed. Reg. 19196).

I. INTRODUCTION

Like Huawei, other commenters agree that protecting the security and integrity of the Nation's communications networks and supply chains is a paramount goal. But the initial comments also confirm Huawei's earlier argument: the proposed rule is neither lawful nor effective for achieving that goal.

A majority of the initial comments are critical of the proposed rule. In addition to Huawei, twelve commenters agree that the FCC should not adopt the proposed rule at the present time, for a variety of reasons ranging from the absence of statutory authority, to the lack of material benefit to national security, to the detrimental effects on the purposes of the USF program and those who

depend on it, particularly in rural areas.[1] Moreover, there is substantial comment that the FCC lacks legal authority in the field of national security even though national security supposedly supplies the justification for the proposed rule, and nearly everyone—even those who purportedly support the rule—acknowledges that the FCC lacks the resources and expertise necessary to assess which suppliers pose national-security threats.[2]

Even the comments that are more favorable to the rule cannot answer the many concerns raised against it. Three such comments express reservations about the NPRM's apparently boundless assertion of authority,[3] while nearly all of the others completely ignore the question whether the FCC has authority to adopt the proposed rule. The principal exception, comments submitted by the Telecommunications Industry Association ("TIA"), simply echo the NPRM's unpersuasive assertions of authority. The pro-rule comments also expose the arbitrary and capricious nature of the proposed rule and further substantiate the likelihood that its costs will vastly outweigh any benefits. Finally, the comments supporting the rule do not address the due process and other constitutional problems inherent in the proposal.

---

[1] *See* Comments of Competitive Carriers Association; Computer & Communications Industry Association ("Computer & Communications"); ITTA—The Voice of America's Broadband Providers ("ITTA–Broadband"); JAB Wireless, Inc. ("Rise Broadband"); Mark Twain Communications Company ("Twain Communications"); NTCA—The Rural Broadband Association ("NTCA—Rural Broadband"); Pine Belt Cellular; Puerto Rico Telephone Company, Inc. ("Puerto Rico Telephone"); Rural Broadband Alliance; Sagebrush Cellular, Inc. ("Sagebrush"); Satellite Industry Association ("Satellite"); and WTA—Advocates for Rural Broadband ("WTA—Rural Broadband").

[2] *See, e.g.*, Competitive Carriers Association Comments at 5, 22; ITTA–Broadband Comments at 3; NTCA—Rural Broadband Comments at 2, 6, 22; Puerto Rico Telephone Comments at 5; Rise Broadband Comments at 5; Sagebrush Comments at 6.

[3] AT&T Services, Inc. ("AT&T") Comments at 3; NCTA—The Internet & Television Association ("NCTA—Internet & Television") Comments at 18; CTIA Comments at 17.

In short, the comments identify many problems with the proposed rule and no adequate solutions. The proposed rule cannot be salvaged, and so Huawei once again urges the Commission not to adopt the proposed rule and to terminate this rulemaking proceeding.

II. THE COMMENTS PROVIDE NO SUPPORT FOR THE FCC'S CLAIMED LEGAL AUTHORITY

It is a fundamental rule that agencies may not take action "in excess of statutory jurisdiction, authority, or limitations." 5 U.S.C. § 706(2)(C). As Huawei and other commenters have argued in their opening comments, the Commission lacks the authority to make national-security concerns determinative in the context of administering the USF program. It follows that the Commission lacks the authority to prohibit USF recipients from using USF funds to buy equipment sold by companies simply because those companies supposedly present some kind of threat to national security.

Huawei explained in detail in its opening comments (at 12-35) why the FCC lacks authority to promulgate its proposed rule. The comments filed by other parties reinforce that analysis. Specifically, the comments confirm that the Commission lacks the statutory authority to treat national-security concerns as dispositive in making USF decisions. *See* Section II.A.1 below. In addition, as explained below, the Commission lacks authority to impose the proposed restrictions under the clear-statement principles governing offers of federal money. *See* Section II.A.2 below. Moreover, the commenters who support the proposed rule have failed to identify any statutory authority for it. Most have not even *attempted* to identify authority for the proposed rule. And the remaining comments do nothing to undermine that conclusion, but in fact reinforce it by raising serious concerns about the broad assertions of authority underlying the NPRM. *See* Sections II.B-II.C below.

A. Other Commenters Agree, and Clear-Statement Principles Confirm, that the FCC Lacks Statutory Authority to Treat National-Security Concerns As Dispositive In the USF Context

1. Many commenters agree that the Commission lacks the statutory authority to treat national-security concerns as dispositive in making USF decisions

As Huawei explained in its opening comments (at 17-25), the Communications Act denies the Commission the power to make national-security determinations dispositive in the context of the USF program. The Act enumerates a list of principles that must guide the Commission's USF decisions, and neither the enumerated principles nor any of the additional principles established by the Commission in accordance with the Act's specified procedures authorize consideration of national-security concerns. What is more, a number of other provisions in the Communications Act *do* include references to national-security concerns—confirming that Congress' refusal to include any similar reference in the universal-service provisions was deliberate. Further, interpreting the Act to empower the Commission to base USF decisions on national-security concerns would violate a multitude of principles that the Supreme Court has articulated—for example, the principle of administrative law and statutory interpretation that Congress should not be presumed to grant an agency the power to make important decisions in an area where it has neither constitutional responsibility nor policy expertise. Huawei Comments 19-25. In short, the Act does not confer on the FCC the authority to make national-security concerns determinative in the USF context.

Many commenters agree with Huawei that the FCC lacks statutory authority to promulgate the proposed rule. For example, the Competitive Carriers Association shows that the proposed rule does worse than simply ignore "the universal service principles set forth in Section 254(b)"; the proposed rule, in fact, "conflicts with" each of those principles. Competitive Carriers Association Comments 16–25. ITTA–Broadband explains that the "sources of authority" that the Commission

has "cobble[d] together" are "at best dubious, if not altogether spurious." ITTA–Broadband Comments 2. And Sagebrush writes that the Commission lacks "the requisite legal authority for the proposed action." Sagebush Comments 6.

Furthermore, when opining on how national-security concerns should be addressed in the USF context, some commenters suggest that other entities, like Congress, the President, and the Department of Justice, are better-positioned to do so. *See, e.g.*, NTCA—Rural Broadband Comments 6-7 (identifying "DHS, DOJ and the FBI" as "critical partners" in "comprehensively assess[ing] and mitigat[ing] supply chain threats"); CTIA Comments 9-13 (noting that the President has asked the National Security Telecommunications Advisory Committee to examine how to improve internet and communications security and the Justice Department has recently created a Cybersecurity Task Force to assess and combat threats to the supply chain). And these comments provide no reason to read the Communications Act to give *the FCC* authority to make national-security concerns determinative *in the USF context*. To the contrary, the comments reinforce Huawei's argument that the text, structure, context, and relevant interpretive principles all show that the Act did not grant the Commission the power to treat national-security concerns as dispositive. Huawei Comments 12-13.

2. The Commission lacks authority to impose the proposed restrictions under the clear-statement principles governing offers of Federal money

Comments expressing concerns about how the proposed rule will affect state and local governments expose yet another reason why the Commission lacks statutory authority to promulgate its proposed restrictions: While Congress may impose certain conditions on the recipients of federal money (like the USF), it must do so unambiguously by statute. *See Pennhurst State School & Hospital* v. *Halderman*, 451 U.S. 1, 17-18 (1981). Agencies cannot impose their own conditions

just because Congress has spoken ambiguously or remained silent. Here, the Communications Act does not impose national-security-based conditions on USF recipients at all, much less in an *unambiguous* manner. Thus, as discussed in detail below, the clear-statement rule articulated in *Pennhurst* and subsequent cases prohibits the Commission's proposed restrictions.

Spending power legislation is "in the nature of a contract: in return for federal funds, [recipients] agree to comply with federally imposed conditions." *Id.* at 17. Congress must express any conditions "clearly" and "unambiguously," however, so that offerees can "exercise their choice [whether to accept the 'contract'] knowingly, cognizant of the consequences of their participation." *Id.* at 17, 25; *see also Gonzaga Univ.* v. *Doe*, 536 U.S. 273, 277, 280 (2002); *Grove City Coll.* v. *Bell*, 465 U.S. 555, 575 (1984) ("Congress is free to attach reasonable and unambiguous conditions to federal financial assistance …."). It is not enough for Congress to "sp[eak] merely in precatory terms." *Pennhurst*, 451 U.S. at 18.

To be sure, an agency may provide reasonable guidance on the scope of conditions that Congress itself has unambiguously imposed in a statute. *See, e.g.*, *Jackson* v. *Birmingham Bd. of Educ.*, 544 U.S. 167, 181-84 (2005) (considering regulations, among other things, in holding that Title IX damages actions encompass retaliation claims); *Am. Hosp. Ass'n* v. *Schweiker*, 721 F.2d 170, 183-84 (7th Cir. 1983) (regulations implemented "unambiguously stated" statutory conditions). That is permissible because, in that circumstance, the *statute* "furnishes clear notice" of the condition, *Arlington Cent. Sch. Dist. Bd. of Educ.* v. *Murphy*, 548 U.S. 291, 296 (2006), thus leaving the agency only to flesh out the details. In such cases, the question is "not *whether* enforceable obligations were created by" the statute, "but rather the scope and interpretation of those obligations." *Am. Hosp. Ass'n*, 721 F.2d at 183.

What an agency may not do, however, is to impose conditions of its own that are not authorized unambiguously by Congress in the first place. *See, e.g., Com. of Va., Dep't of Educ.* v. *Riley*, 106 F.3d 559, 561, 563, 566-67 (4th Cir. 1997) (en banc) (Luttig, J.) ("for the States to be bound by a condition upon the receipt of federal monies, the Congress must have affirmatively imposed that condition in clear and unmistakable statutory terms"); *City of Chicago* v. *Sessions*, 888 F.3d 272, 287 (7th Cir. 2018), *preliminary injunction stayed in part on other grounds*, Order, No. 17-2991 (June 26, 2018) (en banc), Dkt. No. 134; *City of Philadelphia* v. *Sessions*, 280 F. Supp. 3d 579, 646 (E.D. Pa. 2017) (Attorney General's conditions "cannot have been unambiguously authorized by Congress if they were never statutorily authorized"). In other words, "[a]gencies may play the sorcerer's apprentice but not the sorcerer himself." *Alexander* v. *Sandoval*, 532 U.S. 275, 291 (2001); *cf. Gregory* v. *Ashcroft*, 501 U.S. 452, 460, 470 (1991) (plain statement rule applies when an interpretation of federal law could "upset the usual constitutional balance of federal and state powers").

This well-established clear-statement rule bars the Commission from imposing its proposed funding restrictions in the supposed name of national security. As an exercise of Congress' power to spend for the general welfare, the USF is intended, among other things, to extend "public funds" to "help open new worlds of knowledge, learning and education to all Americans." *United States* v. *Am. Library Ass'n, Inc.*, 539 U.S. 194, 212 & n.5, 214 (2003) (discussing E-rate program); S. Rep. No. 105-226, p. 3 (1998) ("The universal service assistance program is a form of subsidy undertaken as part of the spending power of Congress."). Support under the E-rate and Rural Health Care programs, for example, is available to "all public and nonprofit elementary and secondary school classrooms, health care providers, and libraries," 47 U.S.C. § 254(h)(2)(A), to ensure that they "have access to advanced telecommunications services," *id.* § 254(b)(6). But the

statute gives those entities no hint—let alone the requisite unambiguous notice—that their use of USF money might depend on purported national-security conditions. Elsewhere § 254 gives schools and libraries clear notice that they cannot benefit from USF-subsidized internet services unless they maintain compliant internet-safety policies. *Id.* § 254(h)(5), (6), (*l*); *see Am. Library Ass'n*, 539 U.S. at 202-03, 214 (internet condition "is a valid exercise of Congress' spending power"); S. Rep. No. 106-141, p. 8 (1999) ("spending bill" "require[s], as a contingency for receipt of a Federal subsidy, certain measures to restrict children's access to" obscene materials); S. Rep. No. 105-226, at 3 (bill's requirements "attempt to balance the right of States to administer their schools and libraries with the power of Congress to see that federal funds are appropriately used"). Conspicuously absent from the statute, however, is any language—unambiguous or otherwise—conferring authority on the Commission to flesh out conditions based on national security in the USF context. Huawei Comments 12-35; *see also* Section II.A.1 above. That Congress imposed an express funding condition relating to internet-safety policies but failed to create a funding condition based on national security is telling. *See Pennhurst*, 451 U.S. at 23 ("The existence of explicit conditions throughout the Act, and the absence of conditional language in [the relevant provision]," underscore that the relevant provision did *not* contain an unambiguous funding condition.).

Congress' omission, moreover, is hardly surprising. As the comments of the State E-Rate Coordinators Alliance (at 4-5) and American Library Association (at 3-4) make clear—and as the Commission appears to recognize, NPRM ¶¶ 17, 27—schools and libraries are hardly in a position to comply with the Commission's proposed national-security-based conditions on their own. That unachievable burden alone shows that Congress could not have intended for the Commission to proceed in the manner it proposes, rather than entrusting more appropriate agencies to address any

true national-security concerns that may exist in the USF and other contexts. *See* Huawei Comments 17-25.[4]

In short, *Pennhurst*'s principles instruct that, if Congress wishes to impose a funding condition, "it must do so unambiguously." *Pennhurst*, 451 U.S. at 17. And, far from imposing an "unambiguous[ ]" national-security-based funding condition here, the Communications Act makes clear that the Commission has *no authority* to impose restrictions or conditions based on national security in the USF context.[5]

---

[4] It makes no difference that some USF recipients are private rather than public entities. Even if *Pennhurst* applied only to public entities, which it does not, *see Gonzaga*, 536 U.S. at 277 (applying *Pennhurst* to private university); *Grove City Coll.*, 465 U.S. at 575 (private university), a significant portion of USF money is directed to public entities. For example, USAC reports that in 2017 it committed more than $1.8 billion to "school districts," and searches in the USAC's database of "public school" and "public library" recipients in 2017 reveal more than $173 million and $36 million in commitments, respectively. *See* Search Commitments 2017, https://data.usac.org/publicreports/SearchCommitments/Search/SearchByYear/2017 (visited June 13, 2018). Because the clear-statement rule articulated in *Pennhurst* and subsequent cases governs the interpretation of the statute *at least* with respect to public entities, it controls with respect to all entities, even if "other of the statute's applications, standing alone, would not support the same limitation." *Clark* v. *Martinez*, 543 U.S. 371, 380 (2005) ("The lowest common denominator, as it were, must govern."); *see Carter* v. *Welles-Bowen Realty, Inc.*, 736 F.3d 722, 730 (6th Cir. 2013) (Sutton, J., concurring) ("a statute is not a chameleon"); *see also Barnes* v. *Gorman*, 536 U.S. 181, 190 & n.3 (2002) (*Pennhurst* governs interpretation of the Americans with Disabilities Act, even though it "is not Spending Clause legislation," because it mirrors "the Rehabilitation Act, which *is*").

Nor does it make any difference that USAC sometimes disburses USF money directly to service providers. *See* 47 C.F.R. § 54.514(c). As the NPRM acknowledges, the relevant recipients—the "schools, libraries, and rural health care facilities," ¶ 24—are the beneficiaries and owners of the subsidies. *See id.* ¶ 27; *In re LAN Tamers, Inc.*, 329 F.3d 204, 206, 214 (1st Cir. 2003). That functional understanding comports with Supreme Court case law. *See, e.g.*, *Grove City Coll.*, 465 U.S. at 569-70 ("[W]e have little trouble concluding that Title IX coverage is not foreclosed because federal funds are granted to Grove City's students rather than directly to one of the College's educational programs.").

[5] The NPRM (at ¶ 35) relies on *In re FCC 11-161*, 753 F.3d 1015, 1046-47 (10th Cir. 2014), for the proposition that "nothing in [the Communications Act] limits the FCC's authority to place

B. TIA's Arguments Do Not Support The FCC's Claimed Authority

Among the commenters who favor the proposed rule, TIA stands out for trying hardest to identify legal authority for it—but to no avail. TIA's efforts largely just restate the inadequate rationale advanced in the NPRM itself. TIA relies on the same statutory provisions and the same single case as the NPRM. As shown in Huawei's opening comments (at 12-35), as well as below, however, those citations fail to support the notion that the FCC may make national-security concerns determinative in administering the USF program. Nothing in the statutes Congress has written provides that the Commission may treat national-security considerations as dispositive in the USF context, let alone in the manner currently proposed.

As TIA notes, "[v]irtually every provision of the Communications Act or the NTIA Organization Act relating to national defense requires relevant determinations to be made by the President or by Congress." TIA Comments 26-27. In addition, despite its overarching contention that the FCC has authority for the proposed rule, TIA openly concedes that the FCC lacks national security expertise and so "should be careful to avoid making national security judgments of its own." *Id.* at 25. That concession only undermines TIA's argument and, as noted (*see* Section II.A

---

conditions … on the use of USF funds." As discussed in greater detail below, *see infra* Section II.B.2, *In re FCC 11-161* does not purport to give the Commission blanket authority to impose conditions of its own making. The court there relied on the particular language of § 254(c)(1) and express statutory condition in § 254(e) that "[a] carrier that receives [USF] support shall use that support only for the provision, maintenance, and upgrading of facilities and services for which the support is intended," and merely permitted "the FCC to flesh out precisely what 'facilities' and 'services' USF funds should be used for" in light of the policies set out expressly in § 254(b). *See* 753 F.3d at 1046-47. That ruling in no way implies that the Commission can impose conditions of its own, or flesh out any existing statutory conditions based on considerations outside the bounds of § 254(b)'s controlling principles. Moreover, § 254(e) applies to *carriers*; it provides no notice to non-carrier USF recipients.

above), bolsters Huawei's point that Congress could not have intended the FCC to proceed with this type of rulemaking.

1. The statutory provisions invoked by TIA do not support the proposed rule.

Like the NPRM, TIA misplaces reliance on §§ 201(b) and 254 of the Communications Act. Section 201(b) merely grants the Commission general authority to "prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter." 47 U.S.C. § 201(b). According to TIA, the proposed rule "is in the public interest," and so supposedly "advance[s] the principles outlined in Section 254(b)." TIA Comments 24. This simplistic analysis fails for two reasons.

First, it contravenes Supreme Court precedent. The Court has consistently recognized that a statutory reference to "the public interest" is not an open-ended authorization to consider any policy considerations the agency chooses, regardless of its statutory charter or area of expertise. *See, e.g.*, *NAACP* v. *FPC*, 425 U.S. 662, 669 (1976) ("This Court's cases have consistently held that the use of the words 'public interest' in a regulatory statute is not a broad license to promote the general public welfare."); *Nat'l Broad. Co.* v. *United States*, 319 U.S. 190, 216 (1943) ("The 'public interest' to be served under the Communications Act is … the interest of the listening public in 'the larger and more effective use of radio.'"); Huawei Comments 25-27. In the present context, then, the "public interest" that the FCC may consider is dramatically more circumscribed than TIA supposes. For universal service in particular, the Communications Act provides that the public interest consists of the set of enumerated principles expressly codified in § 254(b). The statute says that the Joint Board and Commission "shall base policies for the preservation and advancement of universal service on" those universal-service principles. 47 U.S.C. § 254(b).

The second problem follows from the first: TIA's arguments contravene the principles articulated in § 254(b). As Huawei explained in its initial comments, none of the universal-service principles in § 254(b) includes national security or any remotely similar consideration. Huawei Comments 13-17. Instead, § 254(b) obligates the FCC to focus on the availability, accessibility, and affordability of telecommunications and information services. Apart from a purely conclusory assertion, TIA never attempts to explain how the proposed rule advances these principles. That is presumably because the proposed rule would *jeopardize* the availability, accessibility, and affordability of universal services by restricting competition based on the statutorily unauthorized invocation of supposed national-security concerns.

2. The Tenth Circuit's decision upholding the FCC's authority to impose broadband-related conditions on USF funding does not support the proposed rule.

TIA cannot get around these problems through the USF case law. The lone case that it cites interpreting the relevant statutory provisions, *In re FCC 11-161*, 753 F.3d 1015 (10th Cir. 2014), involved completely different facts, as TIA's description acknowledges. TIA Comments 24-25.

The controversy there centered on the FCC's efforts to fulfill Congress' direction to increase access to broadband internet services throughout the United States. *In re FCC 11-161*, 753 F.3d at 1035-36. To promote extension of broadband networks in unserved areas, the FCC adopted rules requiring USF recipients to offer broadband service upon customers' reasonable request as a condition of receiving USF funds. *Id.* at 1039. As the court made clear, however, and as discussed further below, those rules, which "flesh[ed] out" the statutory condition set out in § 254(e), were based on a reasonable interpretation of the principles set forth *by statute* in § 254(b). Those provisions say nothing about national security. It is therefore unsurprising that TIA ultimately acknowledges the FCC's "determination about the importance of broadband … was easily within the

wheelhouse of the Commission's expertise"—unlike the NPRM's foray into national security assessments. TIA Comments 25.

As noted, *In re FCC 11-161* concerned challenges to the FCC's efforts to condition USF funding on broadband access. The challengers' lead argument rested on § 254(c)(1), which defines "universal service" by reference to "telecommunications services" only, and so the challengers argued that the provision at least implicitly limited the FCC's ability to promote non-telecommunications services using the USF program. That limitation was fatal to the order at issue, in the challengers' view, because the FCC had classified broadband services as "information services" rather than "telecommunications services." *Id.* at 1042. The Tenth Circuit rejected the challengers' invocation of § 254(c)(1) on the ground that "nothing in subsection (c)(1) expressly or implicitly deprives the FCC of authority to direct that a USF recipient … use some of its USF funds to provide services or build facilities related to services that fall outside of the FCC's current definition of 'universal service.'" *Id.* at 1046. "In other words," the court continued, "nothing in the statute limits the FCC's authority to place conditions, such as the broadband requirement, on the use of USF funds." *Id.*

Echoing the NPRM, TIA wrests that last sentence out of context to suggest that the FCC has *unlimited* authority under § 254 to impose conditions on USF recipients. *See* TIA Comments 24; *cf.* NPRM ¶ 35. But the court said nothing of the sort. It concluded only that § 254(c)(1) did not contain the particular limitation that the challengers asserted—*i.e.*, that the FCC's potential objectives must be limited to promoting "universal service." Here, in contrast, § 254(c)(1) is irrelevant. It has no bearing on whether the FCC has authority to make national-security judgments determinative in administering the USF program. Section 254(b), on the other hand, shows that the FCC has no such authority.

Indeed, the Tenth Circuit's ruling that § 254(e) implicitly grants the Commission authority to decide which facilities and services are appropriate for USF funds rests on a crucial statutory limitation: As the FCC conceded, in assessing facilities and services appropriate for USF funds, it is obligated to "achieve the principles set forth in section 254(b) and any other universal service principle that the [FCC] may adopt under section 254(b)(7)." *In re FCC 11-161*, 753 F.3d at 1047. Thus, as the court stressed, the FCC's reading of § 254(e) was "consistent with the directive in § 254(b)" and simply allowed the FCC "to make funding directives that are consistent with the principles outlined in § 254(b)(1) through (7)." *Id.* There was no real dispute over whether the FCC's broadband condition was consistent with § 254(b) because § 254(b)'s universal service principles are not restricted to telecommunication services. On the contrary, the subsection specifically permits the FCC to consider access to "telecommunications *and* information services." 47 U.S.C. § 254(b) (emphasis added). So § 254(b) necessarily includes broadband information services.

At bottom, the Tenth Circuit's decision expressly reaffirms the rule that "the FCC may exercise its discretion to balance the [universal-service] principles against one another when they conflict, but *may not depart from them altogether to achieve some other goal*." *In re FCC 11-161*, 753 F.3d at 1055 (emphasis added). But here, nothing in § 254(b) supports the FCC's attempt to treat national-security considerations as dispositive in resolving USF issues. And it is particularly unlikely that Congress, through its silence, intended to authorize the FCC to dispositively base USF participation on the FCC's analysis of national security threats. After all, as TIA acknowledges, the FCC has no expertise or competence in such matters, and the Act elsewhere expressly raises national-security concerns where they were deemed statutorily relevant. Huawei Comments 17-25.

3. TIA cannot cure the Commission's lack of authority by co-opting other government actors' national-security determinations.

Aware that the FCC has no authority to make its own national security judgments in the context of the USF program, *see* TIA Comments 25, TIA appears to suggest that the problem disappears if the FCC draws its inspiration from national security determinations made by the Executive or Congress in other settings. It does not.

For one thing, the executive and congressional actions cited by TIA do not address the question here: whether schools', libraries', and other USF recipients' use of USF funds to acquire equipment or services of certain companies threatens national security. TIA principally highlights restrictions on government procurement of specified companies' products for the government's own use. *Id.* at 15-16. But even if legislators or agencies find some such products unsuitable for acquisition and use by the government in other contexts, it does not follow that the full range of products covered by the proposed rule are unsuitable for less sensitive uses under the USF.

The situation here is therefore far from that in *Bendix Aviation Corp.* v. *FCC*, 272 F.2d 533 (D.C. Cir. 1959), which TIA cites. There, the Office of Defense Mobilization, acting on behalf of the Executive Branch, specifically requested that the FCC reserve certain frequencies in the spectrum exclusively for government use. *Id.* at 535. The challenger's ultimate quarrel was with that executive action rather than the FCC's decision, and its challenge failed because the court's "review authority extend[ed] only to decisions and orders of the Commission." *Id.* at 538. Here, in contrast, the proposed rule would adapt and extend materially dissimilar policy judgments made elsewhere in the government—to a degree yet to be determined—and, under § 254(b), the FCC lacks any power to do so. In enacting that provision, Congress has told the FCC what factors it "shall" consider in administering the USF program, and national security is nowhere among them.

Moreover, as noted in Huawei's opening comments, FCC's reliance on other government actors' national security determinations would be legally improper for a host of additional reasons. For one thing, it would be arbitrary and capricious for the FCC to rely on a determination that a different agency made at a different time and in a different context. Huawei Comments 42-44. Additionally, such an approach would unlawfully disregard the procedural protections that companies are afforded under the Due Process Clause and relevant statutory provisions. *Id.* at 75-84. Finally, to the extent that the FCC assigns the task of compiling the blacklist to another agency, such outsourcing would constitute an unlawful subdelegation. *Id.* at 81.

C. The Other Comments Supporting The Proposed Rule Confirm The Commission's Lack Of Statutory Authority

Other than TIA, commenters favoring the proposed rule largely ignore the FCC's lack of authority to base USF policies on the FCC's assessment of national security. Most of these commenters say nothing about whether the FCC has statutory authority for the proposed rule.[6]

Two other commenters who neither unequivocally support nor unequivocally oppose the proposed rule, AT&T and NCTA—Internet & Television, raise an important concern about the NPRM's assertion of authority. According to the NPRM, § 201(b) of the Communications Act allows the FCC to promote national security (as the FCC understands it) because doing so serves "the public interest." NPRM ¶ 35. But nothing in § 201(b) or the NPRM's reliance on it is limited to the USF setting. Both AT&T and NCTA—Internet & Television recognize, as NCTA—Internet

[6] Examples include the comments submitted by: the American Library Association; EchoStar Satellite Operating Corporation and Hughes Network Systems, LLC; Motorola Solutions, Inc.; and USTelecom—The Broadband Association.

& Television explains, that "the Commission does *not* have plenary authority to regulate the communications network supply chain." NCTA—Internet & Television Comments 18 (emphasis added). Indeed, *no one* argues that the FCC has authority to regulate national-security-implicating supply-chain risk across telecommunications networks generally.

In light of the fact that Congress did not confer such broad supply-chain authority on the FCC, the next logical question to ask is whether Congress conferred such authority on the FCC only in the USF context. Along these lines, NCTA—Internet & Television argues that any rule that the FCC promulgates in this proceeding should be restricted only to the USF context. *Id.* But it would have been exceedingly strange for the Act to authorize the FCC to address national-security-implicating supply-chain risks in the USF context only—that is, in the context of high-cost and rural areas, schools, libraries, and rural healthcare facilities—but to ignore such risks across telecommunications networks more generally. There is no reason to think—and no basis in the statute to conclude—that Congress implicitly authorized the FCC to address national security risks in the subset of networks supported by the USF, but to ignore such risks in the broader telecommunications networks. This is especially true because, as Huawei has previously established (Huawei Comments 56), USF recipients are very low-risk targets from a national-security perspective. Moreover, the conclusion that Congress did not authorize the Commission to address such risks solely in the USF context is further underscored by the fact that, as AT&T notes (Comments 3), restricting a rule to USF recipients "would potentially distort competition and harm consumers."

At bottom, if AT&T and NCTA—Internet & Television are correct in denying the FCC's plenary authority to impose national-security regulations throughout the field of communica-

tions—and they are, for reasons Huawei has already explained—the NPRM's assertion of authority over the discrete aspect of the communications industry that is funded by USF cannot be correct.

III. THE PROPOSED RULE IS ARBITRARY AND CAPRICIOUS

Huawei's opening comments explain that the proposed rule is arbitrary and capricious under the Administrative Procedure Act ("APA") because it is unduly vague, draws irrational lines, and fails to reflect reasoned decisionmaking. Other comments reinforce each of these points.

A. The Comments Confirm That the Proposed Rule Is Unduly Vague and Offers No Meaningful Guidance to Affected Parties

Huawei has explained that the proposed rule consists of only a single paragraph and fails to provide either a meaningful opportunity to comment on the proposal or a meaningful opportunity to understand the prohibition that the Commission proposes to adopt. Huawei Comments 36. In particular, the NPRM does not define the key term "national security." Nor does it provide any explanation whatsoever as to how to identify, establish, or measure whether a particular company "pos[es] a … threat" or "risk" to "national security."

Other commenters, including some supporters of the proposed rule, have echoed Huawei's concerns. For instance, the American Library Association states that "several of the proposals in the Notice" "will likely cause confusion" and will require "determinations" that are "difficult for providers to make." American Library Association Comments 2. Computer & Communications finds the proposed rule "very unclear." Computer & Communications Comments 6. ITTA–Broadband explains that the proposed rule is "fraught with uncertainty." ITTA–Broadband Comments 6. Twain Communications and Pine Belt Cellular comment that "the proposed rule will result in uncertainty for rural telecommunications companies"—because such companies cannot

"predict which … service providers may be determined in the future to pose a national security threat"—thereby "discourag[ing] such companies from investing additional money and resources into future network expansion and development." Twain Communications Comments 2–3; *accord* Pine Belt Cellular Comments 3–4. And NTCA—Rural Broadband notes that "the Commission's current high-level proposal lacks sufficient definition and detail to enable meaningful analysis or commentary." NTCA—Rural Broadband Comments 7. On the other side of the ledger, not a single commenter argues that the proposed rule is sufficiently well defined to provide adequate notice to potential commenters and adequate guidance to regulated parties.

B. The Comments Confirm that the Proposed Rule Draws Irrational Lines

Huawei has also explained that the proposed rule draws irrational lines and is thus arbitrary and capricious. Other comments underscore Huawei's arguments.

To start, Huawei has explained that the proposed rule improperly targets particular *sellers* rather than particular *equipment*. Huawei Comments 38; Exhibit A, Reply Declaration of Donald Purdy, Jr. ("Purdy Reply Decl.") ¶ 6. Numerous other commenters agree that this approach is irrational.

For example, Competitive Carriers Association points out that "the Commission has not explained why it proposes to target *companies* instead of *products*, when it is the equipment and devices that allegedly create the security risk." Competitive Carriers Association Comments 38. Rise Broadband notes: "There is no evidence, in the *NPRM* or otherwise, that *every single product* manufactured by a particular company poses a national security threat. After due inquiry, it may be determined that there are valid concerns regarding particular components or technologies … but it is unlikely that every single module somehow connected to a particular manufacturer places

the United States at risk." Rise Broadband Comments 5. And NCTA—Internet & Television urges the Commission to "employ a more targeted approach" that focuses on the "specific … equipment items that raise known and identifiable national security risks," rather than adopting "a blanket prohibition on the use of any equipment provided by a blacklisted vendor." NCTA—Internet & Television Comments 12. TracFone Wireless, Inc. ("TracFone"), likewise argues that "applying the proposed prohibition to end-user devices" would be unnecessary given the "minimal risk to supply chain security that such devices may pose." TracFone Comments 3–5.

Taking a different view, TIA urges the Commission to "publish a list of prohibited suppliers." TIA Comments 54. But even TIA cannot bring itself to fully embrace this seller-based approach, as it proposes standards that include a wide range of "*product-specific* criteria," such as "the relevance of a particular product to security within a network" and the nature of the "user" of the particular product. *Id.* at 84 (emphasis added).

Moreover, in April 2013, TIA sent a letter to congressional leaders explaining that, "fundamentally, product security is a function of how a product is made, used, and maintained, *not by whom or where it is made*." Exhibit B, Letter to Representatives J. Boehner, H. Reid, N. Pelosi, and M. McConnell (April 4, 2013) ("2013 TIA Letter") (emphasis added). It advised then that adopting an approach to product security that turns on the identity of the supplier "run[s] the risk of creating a false sense of security," "risk[s] undermining the advancement of global best practices and standards on cybersecurity," "impede[s] the U.S. government's ability to protect itself," "fuel[s] potential retaliation," and "encourage[s] copycat legislation" that "could undermine U.S.-based companies' global competitiveness." *Id.* at 1–2. TIA was right in 2013, and it offers no explanation for its departure from those sound positions.

Huawei has further explained that the proposed rule is arbitrary because it ignores the reality that the supply chain for telecommunications equipment is global, and because it restricts equipment provided by Huawei and ZTE but not equipment made by other companies with equally or more significant ties to China. Huawei Comments 39. TIA agrees that equipment sellers "rely heavily on global supply chains," that "global supply chains that have been built out over decades are critical to the health and competitive standing" of American businesses, and that "any actions by the Commission must account for the critical role of these supply chains." TIA Comments 44. That acknowledgment only underscores Huawei's point: A wide range of companies have manufacturing facilities in China, embed components imported from China, use software written by Chinese programmers, and have other ties to China. Some even have formed joint ventures with the Chinese Government. Huawei Comments 40–41 & n.11. Even if national origin were a rational basis to bar certain equipment—and it is not—neither the Commission nor any commenter has identified a persuasive justification for singling out Chinese telecommunications manufacturers such as Huawei on account of their ties to China, while still overlooking the many other businesses with comparable or even greater ties to China. For example, if ties to China are the relevant consideration, there is no rational explanation for why Huawei is a targeted company, while (1) China Huaxin, a 100% Chinese state-owned company,[7] is not, and (2) Nokia Shanghai Bell, an *affiliate* of China Huaxin under TIA's proposed definition,[8] is not either. To be clear, Huawei is in no way

[7] China Huaxin Post and Telecom Technologies Co., Ltd., *About Us*, http://www.sinohx.com/en/about.aspx (visited June 27, 2018).

[8] *See* Huawei Comments Ex. M, "Nokia Signing a Joint Venture Agreement with China Huaxin to Establish Nokia Shanghai Bell" (noting that China Huaxin will hold almost 50 percent of Nokia Shanghai Bell's shares); TIA Comments 57 (proposing that "affiliates (25% or 10%) … of prohibited companies" likewise be prohibited).

suggesting that Nokia poses a national-security threat or that it should be precluded from selling to USF-funded buyers. Rather, just as Nokia's ties to China do not undermine the safety of Nokia's equipment, Huawei's ties to China also do not undermine the safety of Huawei's equipment. The Commission's failure to recognize this point—and thereby to allow Nokia, but not Huawei, to sell equipment to USF recipients—is arbitrary. Huawei Comments 41.

Next, Huawei has shown the arbitrariness of the methods by which the Commission proposes to identify the sellers to be blacklisted. Huawei explained that the mere fact that another governmental entity has deemed a company a threat to national security in a different context (such as nuclear defense) does not support a finding that the company is also a threat to national security in the USF context. *Id.* at 42. Many other commenters reinforced this point by showing that there is no reason to believe that the USF setting raises uniquely sensitive national-security concerns. *See, e.g.*, Competitive Carriers Association Comments 35; NTCA—Rural Broadband Comments 16. In the meantime, no commenter explained why it would be rational to conclude that a company poses a threat in a less sensitive context merely because Congress or another agency concluded that it supposedly poses such a threat in a more sensitive context. The reason no commenter has explained this is because no rational explanation exists.

TIA essentially concedes as much. Its proposed rule text states—three times—that the relevant criteria should hinge on national-security determinations that were made in the context of "*civilian* federal agencies." *See* TIA Comments, App. (stating that a company should be blacklisted in the USF context if, among other things, it is "prohibited by name as the result of a federal interagency review process established either by statute or by executive order from selling one or more covered communications technology products to one or more *civilian* federal agencies for national security reasons") (emphasis added); TIA Comments 56 ("The Department of Defense

often imposes a higher bar for procurement of certain products. Companies should not be prohibited solely because they have been unable to meet the threshold for procurement by DoD"). Thus, TIA's proposal plainly reveals its understanding that a Department of Defense decision regarding a particular company should not translate to the USF context.

Finally, Huawei has shown that the proposed rule is unconstitutional and arbitrary and capricious to the extent that it discriminates on the basis of national origin. Huawei Comments 44. TIA's comment actually reinforces that invidious discrimination is at work. TIA urges the Commission to blacklist a small group of companies including Huawei, but discourages the Commission from blacklisting other companies that do business in China. The ostensible justification is that these other companies pose a lesser security risk *because* they are "non-Chinese." TIA Comments 45. In other words, TIA seems to equate "risk" with national origin. This disparate treatment is unconstitutional as well as arbitrary and capricious.

C. The Comments Confirm that the Proposed Rule Reflects Irrational Decisionmaking

Huawei has shown, last of all, that the proposed rule fails to reflect reasoned decisionmaking. Huawei Comments 47–53. Other comments highlight some of the key flaws.

First, the other comments show that the Commission is rushing headlong into an area in which everyone agrees the Commission lacks expertise. Virtually every commenter, including virtually every supporter of the proposed rule, agrees that the Commission lacks the expertise to make judgments about whether particular companies pose risks to national security. To list just a few examples: The Competitive Carriers Association emphasizes that "it is ill-advised for the Commission to attempt to make complex national security and foreign policy determinations," which lie "outside the Commission's area of expertise." Competitive Carriers Association Comments 5.

CTIA notes that "the Commission is not well-positioned to determine which suppliers could most readily put … security at risk." CTIA Comments 13. TIA admits that "the Commission should not make its own national security determinations regarding any particular supplier, as it lacks the expertise to do so." TIA Comments 4. These and similar comments confirm the unlawfulness of the Commission's proposed rule. It is arbitrary and capricious for an agency to insist on making policy in a given area when everyone, even supporters of the proposal, acknowledge that the agency lacks competence in that area.

The Commission cannot avoid this problem by relying on determinations made by another agency. As Huawei has explained, the very fact that the Commission lacks the expertise to make national-security policy confirms that Congress never authorized the Commission to rest USF funding decisions on national-security considerations. Huawei Comments 20–21. Even assuming *arguendo* that it had such authority, though, as Huawei has also shown, the Commission may not outsource its statutory assignments to some other entity. *Id.* at 81. Put simply, the Commission may not say, "We have so much expertise in national security that Congress implicitly authorized us to treat national-security concerns as decisive when distributing USF funds," while simultaneously saying, "We have so little expertise in national security that we need to hand off the task of blacklisting suppliers to other agencies."

Second, the comments demonstrate the Commission's failure to account for the wide range of investment-backed expectations that the proposed rule upsets. *See Motor Vehicle Mfrs. Ass'n* v. *State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 48 (1983) (agency action is arbitrary and capricious to the extent it fails to consider "an important aspect of the problem"). By way of example, Huawei has explained the effects of the proposed rule on its own transactions. "Huawei's customers are uncertain as to their ability to purchase Huawei products in the future." Huawei Comments Ex. C,

Dowding Decl., ¶ 33. As a result, "customers have cancelled purchase orders, stopped paying for equipment and services already provided, and suspended projects and contract negotiations." *Id.*; *see also* Competitive Carriers Association Comments, Houseman Decl. ¶ 4 ("When the FCC released its proposed rule, United was in the process of ordering new Huawei equipment…. This project is now on hold."). This unreasonable disruption of existing and impending contracts "has caused huge financial losses to Huawei, resulting in reductions in its U.S. workforce." Huawei Comments Ex. C, Dowding Decl., ¶ 33.

Other commenters have also explained that the proposed rule will have similar effects on the recipients of USF funding. *See* Section IV.B below. Even assuming that the Commission applies the proposed rule only to future equipment purchases and not to equipment purchases already made, the rule would, "as a practical matter," "likely require many carriers to rip and replace equipment purchased from targeted companies." Competitive Carriers Association Comments, Berry Decl. ¶ 11. That is so because "network equipment needs regular servicing and technology upgrades," but using a "hodge-podge" network with preexisting equipment made by one manufacturer and new equipment made by another would raise "interoperability concerns." *Id.*; *see also* Competitive Carriers Association Comments, Beehn Decl. ¶ 5 (discussing "interoperability problems"). Forcing funding recipients to replace existing networks would be "devastating." Competitive Carriers Association Comments, Berry Decl. ¶ 13. For example, one member of the Competitive Carriers Association would face "$410 million in direct, 'rip and replace' costs." *Id.* Another carrier explains that the practical effect of the proposed rule would be to "force [the company] out of business." Competitive Carriers Association Comments, Beehn Decl. ¶ 5. Yet another says that "the FCC's proposed rule threatens [the company's] ability to survive." Competitive

Carriers Association Comments, DiRico Decl. ¶ 4. The Commission's failure to seriously consider these unreasonable effects is arbitrary and capricious.

Third, the comments highlight the Commission's failure to take seriously alternatives to its proposal. "An agency must cogently explain why it has exercised its discretion in a given manner." *State Farm*, 463 U.S. at 48. That means that an agency's "failure to consider … alternatives, and to explain why such alternatives were not chosen, [is] arbitrary and capricious." *Int'l Ladies' Garment Workers' Union* v. *Donovan*, 722 F.2d 795, 815 (D.C. Cir. 1983); *see, e.g.*, *Dist. Hosp. Partners, L.P.* v. *Burwell*, 786 F.3d 56, 59 (D.C. Cir. 2015) ("Nor do we uphold agency action if it fails to consider significant and viable and obvious alternatives").

The comments show that a wide range of alternatives is available to the Commission. There is a broad consensus across the government and the private sector on the need to use a risk-based approach to address cybersecurity. Purdy Reply Decl. ¶¶ 8–12. The NIST Cybersecurity Framework, for example, is an increasingly well-recognized tool adopted by various countries governments and enterprises for assessing and addressing cybersecurity risk; indeed, the President has required that federal agencies use this framework for managing their own cybersecurity risks, *see* NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Apr. 16, 2018) ("NIST Framework"); Executive Order 13800, Strengthening the Cybersecurity of Federal Net-

works and Critical Infrastructure (May 11, 2017), and it is used by 30 percent of U.S. organizations, with that number expected to reach 50 percent by 2020.[9] The most recent version of that framework includes a module specifically focused on managing supply chain risk. NIST Framework 15–17. Moreover, as Huawei and others have explained, the Commission's own Communications Security, Reliability and Interoperability Council ("CSRIC") has recommended addressing supply-chain security issues in telecommunications networks through a risk-based approach, including security-by-design principles and processes, not by blacklisting particular companies. Huawei Comments 49; Rural Broadband Alliance Comments 4. The Commission inexplicably fails even to mention CSRIC's recommendations, much less explain its radical departure from considering them to this new proposed rule. Purdy Reply Decl. ¶¶ 8–12, 15–18.

Building on the NIST and CSRIC approaches, Rural Broadband Alliance has submitted an expert report documenting a variety of steps that could reduce supply chain risks in the telecommunications sector. Rural Broadband Alliance Comments, Ex. 1. And WTA—Rural Broadband urges the Commission to "consider alternatives" such as "an equipment testing regime." WTA—Rural Broadband Comments 7. TIA claims that testing can detect only inadvertent security vulnerabilities, not deliberate ones. TIA Comments 36–38. But while no testing regime will be perfect

---

[9] NIST, *Cybersecurity "Rosetta Stone" Celebrates Two Years of Success* (Feb. 18, 2016), https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success.

Other countries have also endorsed the NIST Framework. *See, e.g.*, Public Safety Canada, *Fundamentals of Cyber Security for Canada's Critical Infrastructure Community* 5 (1st ed. 2016) ("Canadian Public Safety Canada endorses the NIST Framework, developed by the United States' Department of Homeland Security with the National Institute for Standards and Technology (NIST), and acknowledges the relevance and applicability of the NIST Framework in the Canadian context."), available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx.

and detect all vulnerabilities, real-world experience demonstrates that a well-designed testing program is capable of detecting both intentional and unintentional ones. *See* Purdy Reply Decl. ¶ 19; *see generally* Exhibit C, Reply Declaration of Thomas Dowding ("Dowding Reply Decl.") ¶¶ 9–10. Indeed, the industry and various standards bodies have developed best practices, certification requirements, and standards for testing to reduce the risk of vulnerabilities. *Id.* For example, the U.S. government's Committee on National Security Systems ("CNSS") Policy No. 11 provides that commercial off-the-shelf IT products used in national-security systems shall be evaluated under the Common Criteria testing program overseen by the National Information Assurance Partnership.[10]

Risk-based approaches such as those just described have obvious advantages over the FCC's proposal: for example, they would address risks systemically across a range of threat vectors regardless of whether the threat originates in the software or any particular component and where that software or component was made. Purdy Reply Decl. ¶¶ 13–17. And, as the Competitive Carriers Association explains, a risk-based approach would also take into account steps that wireless carriers and ISPs themselves can take, such as the use of sophisticated software to detect cybersecurity malfeasance. Competitive Carriers Association Comments, DiRico Decl. ¶ 3. The Commission has never explained why it is not pursuing these alternatives, which would more systematically address supply chain risks, as opposed to singling out several companies and ignoring the global nature of the supply chain. As the Chief Information Officer of the National Nuclear

[10] CNSS, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products, Policy No. 11 (June 10, 2013), available at https://cryptome.org/2013/07/CNSSP-11.pdf.

Security Administration recently stated, "When we start pulling the onion back on all of the products and services that you have, you're going to find a chip somewhere—let's just be honest about it—from one of the nations we're not happy about using."[11] As a result, "[y]ou can't think about it: 'Well, I'm not going to use that product because it came from China'"; instead, the government should focus on mitigating the risks posed by *any* software or product.[12]

The Commission's failure to rationally consider these alternatives and to explain its reasoning makes the proposed rule arbitrary and capricious. As NTCA—Rural Broadband explains, "[t]aken together, the NIST Cybersecurity Framework and, as applied to the communications sector, CSRIC's follow-up reports, specify a clear path forward. … 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." NTCA—Rural Broadband Comments 12; *see* Purdy Reply Decl. ¶¶ 8–19. The Commission's failure to account for that reality and the departure from its longstanding support of a risk-management approach is arbitrary and capricious.

IV. THE COMMENTS CONFIRM THAT THE COSTS OF THE PROPOSED RULE WOULD VASTLY OUTWEIGH ANY POTENTIAL BENEFITS

An administrative agency ordinarily must review the costs and benefits of a major regulatory proposal before adopting it. No agency may "entirely fail to consider an important aspect of the problem," *State Farm*, 463 U.S. at 43—and cost is usually an important aspect of the problem.

---

[11] Joseph Marks, *Banning software isn't the route to cybersecurity, Nuclear Security Agency official says*, Nextgov (June 28, 2018), available at: https://www.nextgov.com/cybersecurity/2018/06/banning-software-isnt-route-cybersecurity-nuclear-security-agency-official-says/149385/.

[12] *Id.*

As Huawei discussed in its initial Comments (at 54-59), the Commission must perform a rational analysis of costs and benefits as part of its rulemaking process. The Supreme Court has explained: "Agencies have long treated cost as a centrally relevant factor when deciding whether to regulate. Consideration of cost reflects the understanding that reasonable regulation ordinarily requires paying attention to the advantages *and* the disadvantages of agency decisions." *Michigan v. EPA*, 135 S. Ct. 2699, 2707 (2015); *Entergy Corp. v. Riverkeeper, Inc.*, 556 U.S. 208, 232 (2009) (Breyer, J., concurring in part) ("every real choice requires a decisionmaker to weigh advantages against disadvantages, and disadvantages can be seen in terms of (often quantifiable) costs"). The agency must "quantify" the costs or "explain why those costs could not be quantified." *Bus. Roundtable* v. *SEC*, 647 F.3d 1144, 1149 (D.C. Cir. 2011). Further, "too much wasteful expenditure devoted to one problem may well mean considerably fewer resources available to deal effectively with other (perhaps more serious) problems." *Entergy*, 556 U.S. at 233 (Breyer, J., concurring in part). That is why all nine members of the Supreme Court agree that an agency usually violates "established administrative practice" by "ignor[ing] cost." *Michigan*, 135 S. Ct. at 2708; *accord id.* at 2714–17 (Kagan, J., dissenting) ("I agree with the majority—let there be no doubt about this—that [the] regulation would be unreasonable if the Agency gave cost no thought at all … Cost is almost always a relevant—and usually, a highly important—factor in regulation. Unless Congress provides otherwise, an agency acts unreasonably in … ignor[ing] economic considerations"). The Commission appears to acknowledge as much in the current proceeding when it expressly "seek[s] comment on the costs and benefits of [the] proposed rule." NPRM ¶ 32.

When an agency considers cost, it must do so in a "reasonable" way. *Michigan*, 135 S. Ct. at 2711. The Supreme Court (in *Michigan v. EPA*) and the D.C. Circuit (in *Business Roundtable*

v. SEC, 647 F.3d 1144 (D.C. Cir. 2011)) have both rejected analyses that they have deemed inadequate. Both of these Courts have held that an agency acts arbitrarily and capriciously by considering cost—which should be a "centrally relevant factor"—only in "attenuated" and "limited ways." *Michigan*, 135 S. Ct. at 2707, 2711; *see also Business Roundtable*, 647 F.3d at 267 ("By ducking serious evaluation of the costs …, the Commission acted arbitrarily"). Both courts have also ruled that an agency must consider the full range of costs imposed by the rule—"any disadvantage," including but not limited to "economic costs." *Michigan*, 135 S. Ct. at 2707; *see also Business Roundtable*, 647 F.3d at 1151 (Commission's refusal to consider certain costs "is illogical and, in an economic analysis, unacceptable"). And both cases condemn regulatory opportunism through which an agency applies one set of principles when judging the benefits but another when judging the costs of the regulation. *See Michigan*, 135 S. Ct. at 2708 (condemning agency's inconsistent treatment of costs and benefits); *Business Roundtable*, 647 F.3d at 1148–49 ("Here the Commission inconsistently and opportunistically framed the costs and benefits"). Last of all, an agency acts arbitrarily and capriciously by "impos[ing] … costs far in excess of benefits." *Michigan*, 135 S. Ct. at 2711; *see also id.* at 2710 ("costs … disproportionate to benefits"); *Riverkeeper*, 129 S. Ct. at 233 (Breyer, J., concurring in part) ("It would make no sense to require plants to spend billions to save one more fish or plankton … That is so even if the industry might somehow afford those billions"). As discussed in detail below, adopting the proposed rule would violate these legal requirements.

Furthermore, several parties commented on the lack of any meaningful cost-benefit analysis in the NPRM, and the need for a more rigorous analysis of these issues before the Commission decides whether to adopt any rule. *See* Competitive Carriers Association Comments 29-30;

NCTA—Internet & Television Comments 2; Sagebrush Comments 2-5. Indeed, as discussed below, the record generated by the initial comments confirms that the proposed rule would impose massive and unjustified costs on the U.S. economy as a whole, and on rural telecommunications carriers in particular, while failing to generate any meaningful national-security benefits. At a minimum, the proposed rule would limit carriers' ability to service or upgrade existing equipment and would require exorbitant investments to replace networks out of whole cloth. Arguments to the contrary, urged principally by TIA, are logically flawed and unpersuasive.

A. The Proposed Rule Would Impair Competition, Discourage Innovation, and Harm the U.S. Economy

1. The proposed rule would reduce competition and cost the American economy billions of dollars

The market for telecommunications equipment, particularly for advanced mobile network equipment including LTE, is already highly concentrated. Exclusion of even one or two major suppliers from this market would significantly increase this concentration, reduce competition, and likely result in increased prices. Because of the key role of the telecommunications industry in the U.S. economy, these increased prices would be felt by nearly all consumers nationwide, even if the direct effect of the rule was limited to USF recipients.

Pushing Huawei and other similarly-situated companies out of the U.S. market would contravene the principle of Chairman Pai's regulatory philosophy that "[c]onsumers benefit most from competition, not preemptive regulation."[13] As the record demonstrates, carriers and ultimately consumers have benefited substantially from the lower prices, better products and better services

[13] https://www.fcc.gov/about/leadership/ajit-pai?qt-leadership_tabs=0#qt-leadership_tabs.

enabled by Huawei's presence in the U.S. market. A direct benefit of competition is cost saving. Exhibit D, Reply Declaration of Allan L. Shampine ("Shampine Reply Decl.") ¶¶ 12, 15.

Huawei is not a low cost 'substitute' supplier. Rather, it is a global leading supplier with pioneering technologies and often times offers a premium price in other countries. Huawei Comments Ex. C, Dowding Decl., ¶¶ 25-26. Huawei's economic contribution cannot be overstated, despite its higher price. In order to compete with Huawei's premier product quality, its competitors often have to offer lower prices. *Id.* at ¶ 27. *See also* Shampine Reply Decl. ¶ 12.

In the U.S. market, restrained competition by companies likely to be targeted under the proposed rule has already resulted in a higher average price than other countries and regions. Huawei Comments Ex. C, Dowding Decl., ¶ 25. As a consequence, Huawei's prices are notably lower in the U.S. compared to its competitors, providing a substantial benefit to those carriers who do entertain bids from Huawei. U.S. carriers could enjoy significantly reduced costs if Huawei were given full access to the market. Shampine Reply Decl. ¶ 15. Looking at mobile carriers alone, the savings of the largest four U.S. carriers would amount to $7.5 billion annually, and the total saving for the North American economy in the period of 2017 to 2020 could be at least $20 billion if Huawei were allowed to freely access the market.

This economic cost is significant not just for its first-order effects, but also its indirect effects on the American economy. The competitors of the targeted companies, which directly benefit from insufficient competition, are likely transferring their profits outside of the U.S. to finance their price competition with the targeted companies in foreign countries. *Id.* at ¶ 11 (noting average selling price of the non-targeted companies is higher in the U.S. than other regions). The devastating consequence of such a result is not only the high financial burden that would frustrate investment, but also the American economy would effectively be funding foreign economies in

developing their telecommunications infrastructure, driving their technology advancement, and helping them to compete with the U.S., all at the cost of American consumers who ultimately pay through their phone bills. Indeed, as various reports show, American consumers are paying higher bills[14] for lower network speed.[15] If this situation is allowed to continue, the technological leadership of American could be given away in international competition.

2. The proposed rule would deny Americans access to Huawei's market-leading technology.

Recognized by the industry across the U.S. and the rest of the world, Huawei is *the* leading supplier in key telecommunications markets. A Huawei customer noted that "[Huawei was] the only company manufacturing equipment that allowed United to fully utilize its spectrum holdings. The technical solution offered by Huawei was superior to other equipment manufacturers." Competitive Carriers Association Comments, Houseman Decl. ¶ 3. For example, in 2017 GlobalData rated Huawei as the "Leader" for 2G/3G Radio Access Network, LTE, and Mobile Packet Core. In other reports of the same period, GlobalData only rated Nokia "Very Strong" in those areas, and only rated Ericsson "Very Strong" in LTE RAN.[16] Cisco didn't even get a rating for

---

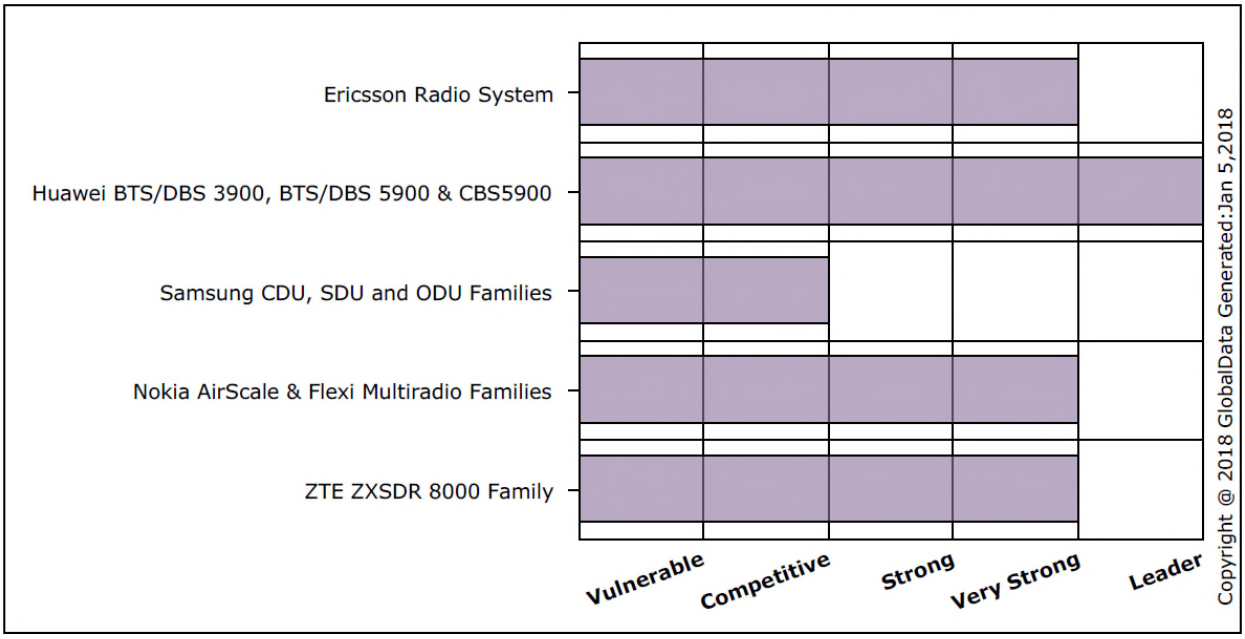
[14] For example, an analyst report shows that, for a monthly price of approximately US $50, AT&T and Verizon offer 1 GB and 2 GB data plans in the U.S., while Orange offers a 20 GB plan in Spain and 30 GB (with an iPhone 7) in France, and Vodafone offers 40 GB in the U.K. Analysys Mason, *Mobile handset data pricing benchmark*, July 2017. *See, e.g.*, https://www.att.com/shop/wireless/data-plans.html; https://www.sprint.com/shop/plan-wall/?INTNAV=LeftNav:Shop:Plans#!/?plan=individual; http://tiendaonline2.orange.es/store/tarifas/contrato; https://boutique.orange.fr/doc/contrat4803.pdf; https://www.vodafone.co.uk/shop/bundles-and-sims/sim-only-deals/.

[15] Huawei Comments Ex. C, Dowding Decl. ¶ 28.

[16] Gubbins, Ed, GlobalData, Huawei - Mobile Access, November 15, 2017, Nokia - Mobile Access, February 20, 2018, Ericsson Radio System, October 31, 2017.

2G/3G/LTE Radio Access Network and only rated "Very Strong" for Mobile Packet Core and "Competitive" for Small Cells.[17]

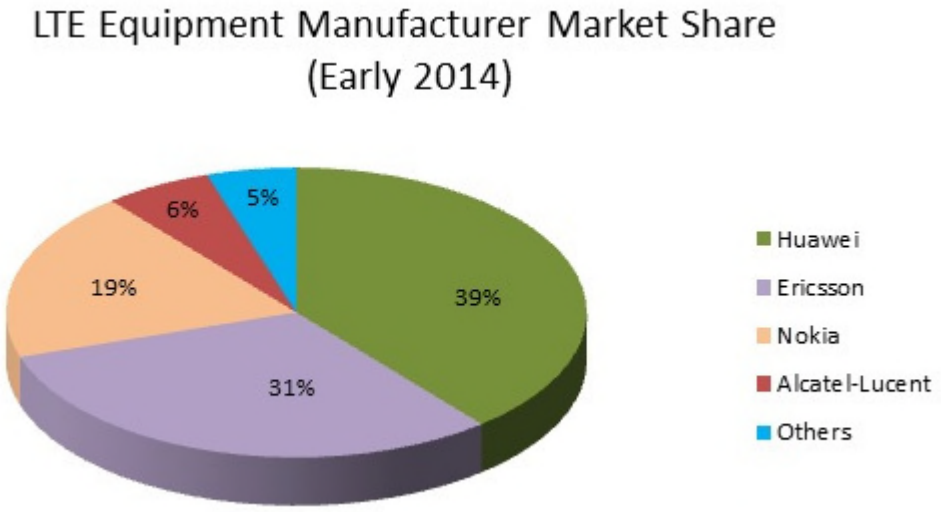
For LTE systems specifically, a GlobalData report shows Huawei is the only "Leader" in the field.[18]



[17] Gubbins, Ed, GlobalData, Cisco - Mobile Access, October 30, 2017.

[18] Gubbins, Ed, GlobalData, LTE RAN: Competitive Landscape Assessment, November 15, 2017.

In terms of market share, despite having limited access to the U.S. market, Huawei is already a world leader of 4G/LTE infrastructure:[19]



When it comes to the next generation wireless technology, or 5G, Huawei's leading position was even more distinguished. Huawei demonstrated the world's first live ultra-high-definition (UHD) IPTV over 5G fixed wireless access (FWA) with a chipset based 5G millimeter wave CPE in October 2017,[20] launched the first commercial 5G terminal device based on its own chipset,[21] and has played a leading role in 5G standardization.[22]

---

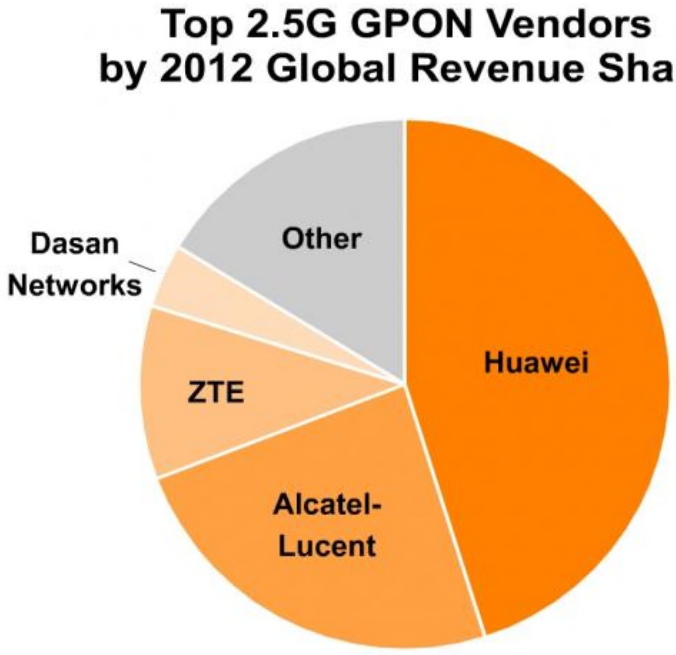
[19] Gunjan Indrayan, *Wireless telecom infrastructure market worldwide – Trends and developments* (Sept. 2, 2014), https://wirelesstelecom.wordpress.com/2014/09/02/wireless-telecom-infrastructure-market-worldwide-trends-and-developments/.

[20] Guy Daniels, *Huawei launches 5G microwave bearer and trials 4K over 5G FWA*, Telecom TV (Oct. 27, 2017), https://www.telecomtv.com/content/5g/huawei-launches-5g-microwave-bearer-and-trials-4k-over-5g-fwa-16124/.

[21] Corinne Reichert, *MWC 2018: Huawei unveils first 5G customer premises equipment* (Feb. 25, 2018), https://www.zdnet.com/article/huawei-unveils-first-5g-customer-premises-equipment/.

[22] Newley Purnell and Stu Woo, *China's Huawei Is Determined to Lead the Way on 5G Despite U.S. Concerns*, Wall Street Journal (March 30, 2018), https://www.wsj.com/articles/washington-woes-aside-huawei-is-determined-to-lead-the-way-on-5g-1522402201, accessed June 27,

Unlike some suppliers focused in limited areas in telecommunications markets, Huawei has a wide spectrum of success across all key areas. For example, in Ovum's report for broadband access market, Huawei holds 36% of the share, more than double of the share of the second largest supplier – Nokia.[23] Infonetics reported in 2013 that Huawei is a 'perennial leader' in the overall broadband aggregation market:[24]



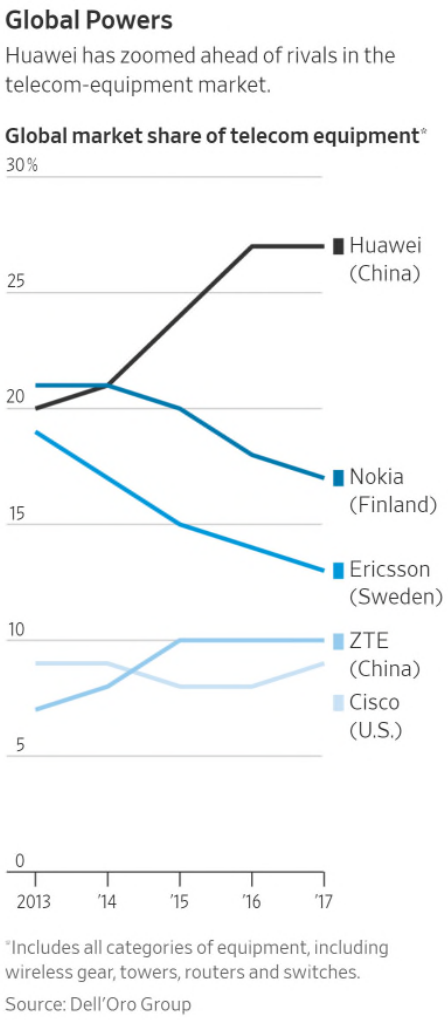
© Infonetics Research, *PON, FTTH & DSL Aggregation Equipment & Subscribers Quarterly Market Share, Size & Forecasts*, Feb. 2013

2018 ("Purnell and Woo"). *See also* Signals Research, Analyzing Cellular Standards Leadership Through A Different Lens, May 21, 2018, http://signalsresearch.com/issue/standing-on-our-5g-soapbox/.

[23] Jaimie Lenderman, Ovum, Market Share Report: 4Q17 and 2017 FTTx, DSL, and CMTS/CCAP, March 28, 2018, https://ovum.informa.com/resources/product-content/spt002-000062.

[24] Alan Weissberger, Infonetics 2012 review & 2013 forecasts for PON, FTTH, DSL Aggregation + Cable Broadband markets (Feb. 26, 2013), http://techblog.comsoc.org/2013/02/26/infonetics-2012-review-2013-forecasts-for-pon-ftth-dsl-aggregation-cable-broadband-markets/.

Yet another firm, Dell'Oro Group, reports that Huawei has been the leading supplier for wireless gears, towers, routers and switches since 2015.[25]



Indeed, the proposed rule would effectively force all American carriers to pay premium prices to get second class products and services. Given the foundational role of the telecommunications infrastructure in the American economy, the inability of carriers to obtain the best technology would trigger a chain reaction, hindering innovation and development across all related

[25] Purnell and Woo, *supra* note 22.

industries. GSMA estimates mobile technologies and services will contribute $1 trillion to North American GDP and more than 2.5 million jobs by the end of the decade.[26] The U.S. cannot afford to become the only country in the world that lacks access to the best communication technologies.

B. The Proposed Rule Would Impose Substantial Costs on Rural Carriers and Other USF Recipients by Restricting Servicing or Upgrades of Existing Equipment, and Imposing Burdensome Compliance Obligations

1. The proposed rule would result in higher prices for rural carriers due to reduced competition

The impact of the proposed rule would be felt especially hard by rural carriers who are dependent on Universal Service Fund support, and by their customers. The effect of the proposed rule on competition in an already limited equipment supplier market is one of the primary concerns expressed in the record. As the Competitive Carriers Association explains, pushing out the targeted, lower-cost providers who serve small carriers would remove "a key constraint on pricing." Competitive Carriers Association Comments 6; *see also* Shampine Reply Decl. ¶ 13 (stating that firms benefit from Huawei's presence in the marketplace even when they do not purchase from Huawei due to competitors developing bids with Huawei's presence in mind).

The proposed rule—if adopted—would have the effect of reducing the overall supply of equipment while simultaneously increasing the demand for equipment from higher-cost providers, driving their prices even higher. Competitive Carriers Association Comments 6; *see also id.*, Berry Decl. ¶ 10 (noting that eliminating lower-cost providers from this market will decrease supply

[26] GSMA, The Mobile Economy – North America 2017 at 4, https://www.gsmaintelligence.com/research/?file=b0cf4f71cb2d035f429d9de8ca4fc72e&download.

without a corresponding decrease in demand and costs will rise). NTCA—Rural Broadband similarly recognizes that a substantial narrowing of the scope of products and services available to rural operators will increase costs for remaining "approved" equipment. NTCA—Rural Broadband Comments 21. Individual small rural carriers with experience working with the targeted companies and other vendors agree.

Huawei's U.S. customers chose Huawei for its affordable cost, premium service, and technology superiority. Some supporters of the proposed rule, such as TIA, ignore the real-world experience of these customers in arguing that alternative suppliers can replace all of the capabilities of the potentially restricted equipment and that "no current recipient of USF support in any of the Commission's universal service programs would be stuck without multiple options." TIA Comments 72. However, the Rural Broadband Alliance notes that its carrier members have stayed in business in part precisely because they have purchased equipment from Chinese manufacturers at price points not available from the other major vendors. Rural Broadband Alliance Comments 3. *See also* USTelecom Comments 15 (stating that "it is commonly understood that equipment from [the targeted companies] is often available at costs substantially below that of other equipment vendors"). For example, Twain Communications indicates that it chose to deploy Huawei equipment in its network because of the affordability and reliability of Huawei equipment in comparison to other vendors used by large providers, which Twain Communications found to be prohibitive. Twain Communications Comments 4-5. United Telephone Association, Inc. ("United") uses Huawei equipment because "Huawei was by far the most cost effective." Competitive Carriers Association Comments, Houseman Decl. ¶ 3. James Valley Telecommunications explains that using Huawei resulted in a 40 percent savings versus the next most cost-effective option. *Id.*, Groft Decl. ¶ 3.

The record reveals not only that the targeted companies often provide more cost-effective solutions, but also that in some cases the targeted companies were "effectively the *only* available providers of products and services" to small carriers. *Id.* at 23 (emphasis in original). WTA—Rural Broadband explains that one of its members could not even obtain a price quote from a Huawei competitor because the vendor said that a small company "would be unable to afford them." WTA—Rural Broadband Comments 4. *Cf.* TIA Comments 72 (stating that potential removal of one or two suppliers would not "appreciably alter" USF recipients' access to choices). Additionally, even if larger vendors were interested in meeting the needs of small rural carriers, existing contracts may prevent larger vendors from resolving small carriers' concerns. Some of the larger vendors who would remain in the marketplace have "most favored nation" clauses in their purchase contracts with carriers serving large urban areas which effectively prevent those vendors from offering discounted rates to rural carriers. Competitive Carriers Association Comments, Berry Decl. ¶ 8. Such clauses that were meant to reduce cost actually end up increasing costs for rural carriers due to the lack of competitive pressure on vendors. This real-world experience of small rural carriers, reflected in the record, demonstrates that eliminating the targeted companies from the market will reduce competition, making it much more difficult for small carriers to survive going forward, even before factoring in the substantial costs of replacing existing equipment discussed further below.

Notwithstanding the unsupported suggestion that other options might *theoretically* exist in the market, small carriers have chosen to use Huawei equipment not just for the lower cost in comparison to other major vendors but for the higher levels of customer service that Huawei provides. Rural carriers have experienced first-hand that Huawei is more attentive to their needs than other service providers and often performs installations and repairs more quickly and reliably.

Competitive Carriers Association Comments 8. For example, NE Colorado Cellular d/b/a Viaero Wireless ("Viaero") uses Huawei for approximately 80% of its network equipment because Huawei was the most cost-effective option and offered the most reliable product and excellent customer service. *Id.*, DiRico Decl. ¶ 3.

Numerous commenters state that the uncertainty created by the proposed rule is already resulting in innovation costs in the form of delayed and reduced network investment. Competitive Carriers Association explains that its members have already decreased capital investments in the first quarter of 2018 in large part due to anticipated tighter restrictions on carriers' access to equipment and services provided by certain foreign companies. *Id.* at 11-12; *id.*, Berry Decl. ¶ 12. One Competitive Carriers Association member expects to invest just $10,000 in network expansion in the first quarter of 2018, a slim fraction of its previous investments of more than $5 million on average per year since 2012. *Id.* at 12. United explains that the uncertainty created by the proposed rule has forced it to freeze all capital investment in its 600 MHz wireless network expansion and that United would be forced to scrap its existing plans and explore more-costly alternatives if the proposed rule is adopted. *Id.*, Houseman Decl. ¶ 5. Because of the uncertainty presented by the proposed rule and other possible governmental restrictions on Huawei, James Valley Telecommunications has restricted investment in its wireless network until the uncertainty passes. *Id.*, Groft Decl. ¶ 6.

Union Telephone Company d.b.a. Union Wireless ("Union") also explains that it has already halted critical projects and significantly slowed down capital investment in network expansion because of the uncertainty created by the proposed rule, including its investment in IP Multimedia System necessary for 4G VoLTE, which will be delayed until late 2019 or 2020. *Id.*, Woody Decl. ¶ 6. Competitive Carriers Association also explains that one of its members will halt

deployment in areas where the service from the incumbent wireline carrier is unavailable or inadequate and another member has halted deployment for "numerous additional coverage areas." *Id.* at 12. The Commission should not ignore the costs to consumers with respect to decreased service coverage and reduced investments in network expansion that the record demonstrates are already resulting, and are likely to continue, if the proposed rule is adopted.

The record also indicates competition in the downstream consumer wireless market will also be undermined due to decreased coverage or small rural carriers being forced out of the wireless business as a result of the proposed rule. For example, Sagebrush predicts that it would need to scale back its network from 161 cell sites to just 55 cell sites (*i.e.*, by approximately 11,700 square miles) if it were to lose universal service support associated with the Huawei equipment in its network. Sagebrush Comments 3. As Sagebrush notes, many of the areas that would experience reduced coverage from network coverage reductions are currently unserved by competing carriers. *Id.* Even areas that enjoy competition from more than one wireless carrier are likely to lose a competitive option. *Id.* at n.2. *See also* Competitive Carriers Association Comments, Beehn Decl. ¶ 5 (stating that the costs of replacement equipment would force SI Wireless out of business and leave its rural customers with less competitive alternatives); Ex Parte Letter from Joseph Franell, CEO and General Manager, Eastern Oregon Telecom, to Marlene H. Dortch, Secretary, FCC (filed June 26, 2018) (urging consideration of the negative effects to rural broadband deployment that would result from a total ban on Huawei equipment).

2. The proposed rule will strand investment by precluding carriers from servicing or upgrading existing equipment

Even if the proposed rule does not expressly mandate that existing equipment be removed from the network, commenters agree that there will inevitably be retroactive effects because the

proposed rule prohibits the expenditure of USF funds on replacement equipment, upgrades, maintenance, service, and support provided by the targeted companies. Competitive Carriers Association Comments at 33. As WTA—Rural Broadband accurately states, although equipment may already be installed, continued funding is necessary for maintenance and upgrades to the equipment through its normal lifespan. WTA—Rural Broadband Comments 6. Additionally, if the proposed rule is adopted, some small telecommunications providers will lose nearly all of the value of long-term service arrangements they have with Huawei or another targeted company. For example, one WTA—Rural Broadband member spent more than $25 million on Huawei equipment for its wireless network and expects to continue using the Huawei equipment for at least five to seven years in line with a maintenance agreement between the carrier and Huawei through 2021. *Id.* at 4. Huawei agrees that the inability for carriers to efficiently maintain and service their existing equipment will destroy much or all of the value of equipment already in place, and being made to rely on inadequate maintenance services from other providers is likely to result in more frequent and longer service outages. Competitive Carriers Association Comments 31-33.

Additionally, rural carriers would have serious long-term interoperability concerns if they were to continue using existing equipment from any companies that are ultimately blacklisted in conjunction with newer equipment from different manufacturers. Pine Belt Cellular Comments 6. As a result, some small carriers are likely to perceive no choice but to take a "rip-and-replace" approach to compliance with the proposed rule. Competitive Carriers Association Comments 9 (stating that the only practicable solution for most carriers will be to "rip-and-replace" existing equipment with new equipment due to the uncertainty regarding interoperability). The proposed rule could result in the need for its rural carrier members to "tear out roughly $1 billion worth of gear currently used to provide mobile voice and broadband in America's rural areas well before

the gear reaches its useful life span and can be depreciated." Rural Broadband Alliance Comments 6. However, regardless of whether rural carriers ultimately adopt a "rip-and-replace" or "mix-and-match" approach to compliance, significant research and development costs will necessarily need to be absorbed somewhere in the market. Competitive Carriers Association Comments 10.

Whether due to inability to service existing equipment, or inability to integrate other manufacturers' equipment into an existing network, carriers who have purchased Huawei equipment face potentially devastating costs if the rule is adopted as proposed. As Competitive Carriers Association notes, the Commission has not even attempted a preliminary estimate of these costs. *Id.* at 32. Huawei agrees that requiring providers to cover the costs of compliance would effectively be "forcing them to reimburse substantial portions of their federal funding." Rise Broadband Comments 7. The Commission need look no further than the record to see that the costs imposed by the proposed rule on rural carriers would be "possibly devastating." Twain Communications Comments 6.

For example, one Competitive Carriers Association member estimates that replacement will require expenditure of nearly $310 million for a new core and related equipment, an additional $60 million in costs for services and maintenance, and a loss of approximately $40 million in roaming revenue from larger carriers during the transition to new equipment. Competitive Carriers Association Comments 11. Pine Belt Cellular estimates that its costs to replace equipment and costs from foregone revenue during the transition will be between $7 million to $13 million. Pine Belt Cellular Comments 6-7. Sagebrush similarly predicts substantial costs and other negative impacts of compliance with the proposed rule on its ability to continue serving its rural customers. In total, Sagebrush expects that a cost-prohibitive $57 million will be necessary to replace its 3G/LTE Huawei network, which includes costs for installation and higher costs of materials, support, and

upgrades going forward. Sagebrush Comments 2; Competitive Carriers Association Comments, Kilgore Decl. ¶ 3. Regardless of whether it chooses to forego universal service support or spend tens of millions to comply, the parent of Sagebrush is concerned that either choice for complying with the proposed rule places its viability in jeopardy. *Id.* at ¶ 6.

Union estimates that replacement of its network would cost approximately $340 million in direct spending and that the transition from its Huawei-based network would take approximately 5 years, resulting in approximately $26 million annually in foregone roaming revenue. Competitive Carriers Association Comments, Woody Decl. ¶ 4. In addition to the replacement costs and foregone roaming revenue, Union anticipates an increase in costs for services from a new supplier of $2 million annually and an annual loss of approximately $20 million in USF support while it continues to engage with Huawei during the transition. Union states that either of its available choices (*i.e.*, to forego universal service support or shoulder more than $300 million in compliance costs) will put its survival into serious question. *Id.* at ¶ 7.

Viaero anticipates costs in excess of $300 million to replace its existing equipment, including approximately $75 million for a replacement core and $60 million for installation. Competitive Carriers Association Comments, DiRico Decl. ¶ 4. During installation, Viaero would forego as much as $50 million in roaming fees from national carriers. Viaero would also need to find a new vendor to service its equipment, which it estimates will cost approximately $4 million more annually than Viaero currently pays. In total, Viaero expects approximately $410 million in direct costs and $4 million in additional annual servicing costs. *Id.* The proposed rule will require Viaero to decide whether to incur compliance costs of $410 million in upfront costs or forego critical USF support and Viaero will struggle to stay afloat. *Id.* at ¶ 7.

James Valley Telecommunications estimates the compliance costs associated with replacing Huawei equipment at $5,000 per affected customer. Competitive Carriers Association Comments, Groft Decl. ¶ 4. James Valley Telecommunications explains that it can forego USF support, which it sees as essential to maintaining its existing network and deploying 5G, or continue to accept USF funds and spend millions of dollars to comply with the proposed rule. *Id.* at ¶ 7. James Valley Telecommunications says that its customers will "certainly experience increased fees if the costs imposed by the proposed rule cannot be recouped through the USF or other sources of revenue." *Id.* at ¶ 5.

3. The proposed rule would undermine the goal of universal service

In addition to the burden of compliance costs and the economic harm due to reduced competition, the impacts of the proposed rule are likely to undermine the Commission's universal service goals in several ways. ITTA–Broadband appropriately points out that increased equipment and services costs incurred by carriers reliant on USF are likely to increase overall demand on the fund. ITTA–Broadband Comments 5. These costs will combine with cuts in USF support overall and will translate into higher rates for consumers, increased customer churn, and ultimately additional harms for carriers. Competitive Carriers Association Comments 7. The proposed rule could also call into question the accuracy of the Alternative Connect America Model and budget control mechanism used to calculate universal service support for small rural carriers. ITTA–Broadband Comments 5-6.

Furthermore, although TracFone's comments avoid wading into the substantive aspects of the proposed rule, it expresses concern that the proposed rule goes too far in practical application because USF supports not just network infrastructure used by carriers or E-Rate and Rural Health

Care support recipients but also low-income consumers through the Lifeline program, many of whom rely on end-user devices, some manufactured by companies that may be blacklisted. TracFone notes that if the proposed rule applied across the board to all USF programs, Lifeline participants would be unable to use more affordable—and in many cases, free—handsets despite the fact that USF subsidizes the service rather than the device. TracFone Comments 4-5.

C. TIA's Arguments That Costs Would Be Limited Are Unfounded

TIA cautions the Commission to proceed carefully, in recognition that the rule could potentially raises costs for telecommunications vendors and invite foreign retaliation. TIA Comments 9. But TIA fails to take accurate stock of just how substantial those costs are, instead offering a number of ineffectual guidelines to "tailor" the rule and disregarding basic economic principles of competition.

1. Cost of U.S. Government intervention in the marketplace

As discussed in Sections IV.A and IV.B above, the proposed rule would impose significant costs on U.S. carriers and in turn U.S. consumers, many of whom live in rural and remote areas where telecommunications offerings are already sparse. TIA's proposed "tailoring" provides no meaningful way to mitigate these costs. Moreover, TIA fails to address the potential harm of the proposed rule on foreign relations and international trade. TIA has long recognized the repercussions of U.S. government intervention in a marketplace where global companies are involved. For example, in 2013, the U.S. House of Representatives contemplated enacting a provision barring certain government agencies from acquiring information technology (IT) systems produced, man-

ufactured, or assembled by Chinese entities unless authorized government staff undertook a cybersecurity risk assessment.[27] A number of trade associations, including TIA, urged the U.S. to "ensure similar language is not included in other legislative vehicles." 2013 TIA Letter 1. Specifically, the trade associations argued that "[a]t a time when greater global cooperation and collaboration is essential to improve cybersecurity, geographic-based restrictions in any form risk undermining the advancement of global best practices and standards on cybersecurity." *Id.* This point is no less salient today.

TIA's comments also acknowledge that "open markets that enable export growth are essential for the continued dynamism of the U.S. telecom sector" and urge the Commission to accordingly "explain clearly that any restrictive actions it may take would be based solely on a narrow national security justification." TIA Comments 40. But merely *making* a statement about why a rule is promulgated does not necessarily make it true. Certainly, TIA points to a number of U.S. government concerns about the Chinese and Russian governments, including the same Chinese law that the Commission misinterpreted. *Id.* at 11-14. But aside from the location of Huawei's headquarters, neither TIA nor the Commission has proffered any rationale for why Huawei, a global company with substantial presence in all countries allied with the U.S., specifically poses any national security threat. The Commission cannot show that the proposed rule is based on a "narrow national security justification" based on fact—because it is not; and no company or association has presented fact-based evidence of any alleged security threat(s) posed by Huawei products.

---

[27] H.R. Res. 933, 113th Cong. (2013).

2. Harm to competition

At the outset, TIA's enthusiasm for a blanket ban of the targeted companies must be questioned. The TIA is accredited by the American National Standards Institute ("ANSI") to develop voluntary, consensus-based industry standards for a wide variety of Information and Communication Technologies ("ICT") products.[28] As a standard setting organization, its members consist a wide range of suppliers of ICT products, who are essentially competitors of each other by nature. Despite Huawei and ZTE's status as TIA board members, TIA Comments noted, "[Huawei and ZTE] do not have access to the Public Policy Committee or to any of its internal communications or deliberations, and so did not influence these comments." TIA Comments 1. Thus, it is reasonable to infer that TIA's Comments instead were influenced by the *competitors* of the targeted companies. The proposed rule will directly benefit these competitors, which can increase their prices and market shares without having to deliver better products and services. TIA virtually twists itself into a pretzel arguing, on the one hand, that Commission action should be "narrowly tailored," there should be a high threshold for any blacklist, and that due process should be respected; but, on the other, that the Commission should immediately blacklist any company that has been prohibited by Congress from providing any type of product to any civilian Federal agency for national security reasons.

Substantively, TIA wrongly asserts that USF recipients would continue to benefit from a competitive marketplace if the proposed rule is enacted. In support, TIA states that Huawei products "reportedly make up less than one percent of the equipment in American cellular and landline

---

[28] Telecommunications Industry Association, https://en.wikipedia.org/wiki/Telecommunications_Industry_Association, accessed June 24, 2018.

networks today" and itemizes various products available as replacements for Huawei equipment. *Id.* at 71-76. But TIA's laundry list of substitute suppliers is misleading. For one, TIA lumps together suppliers serving entirely different product markets, creating a misperception that they are substitutes to each other. Shampine Reply Decl. ¶¶ 5-9. For example, Cisco has no macro base station product, and can't offer its small cell base station as a substitute for a Huawei macro base station installed in a tower covering an area of 4 km.^{2} Likewise, Ericsson, with no core router products, can't offer its optical transmission product as a substitute for a Huawei core router exchanging internet traffic between two cities. While Huawei is a prominent supplier in all the relevant markets TIA lists, none of the companies TIA lists has the same strength and breadth of businesses. *See* Section IV.A.2 above; *see also* TIA Comments 73-75. Furthermore, many of TIA's listed suppliers are, unsurprisingly, TIA members who would financially benefit from, and therefore have a vested interest in, excluding competitors by regulatory *fiat*. These include some members with substantial ties to the Chinese government, such as through joint ventures with Chinese state-owned telecommunications companies.

More importantly, TIA appears to misunderstand how competitive harm occurs to begin with. For example, TIA overstates the relevance of Huawei's comparatively small market share in the U.S., failing to recognize that Huawei can be competitively significant to its competitors, if they want to protect their market shares from being reduced by Huawei's competitive presence in the market. Shampine Reply Decl. ¶¶ 12-13. Carriers that never utilize Huawei equipment nevertheless benefit from Huawei's mere presence in the market. *Id.* at ¶ 13. TIA's emphasis on Huawei's market share in the U.S. is further misplaced because it fails to assess *where* Huawei equipment is primarily used. While large, Tier 1 carriers may not heavily rely on Huawei's equip-

ment, Huawei holds disproportionate market concentration in rural areas with relatively poor wireless and internet access. *Id.* at ¶ 2. As discussed previously, numerous carriers providing critical services to remote areas of the U.S. rely on Huawei equipment and have enumerated the specific costs, financial and otherwise, that the proposed rule would impose. *See, e.g.*, Section IV.B above; Competitive Carriers Association Comments 10; Rural Broadband Alliance Comments 6; Sagebrush Comments 2-3; NTCA—Rural Broadband Comments 21.

TIA also incorrectly assumes that loss of competition is unimportant as long as some alternate equipment *can* be supplied, without analysis of the basic economic question whether that equipment will continue to be supplied at reasonable, competitive prices and technologies. To the contrary, the available evidence consistently demonstrates that Huawei's presence in the U.S. marketplace disciplines prices to some extent despite its lower share. Shampine Reply Decl. at ¶¶ 12-13. In fact, Huawei's presence in the market has already resulted in a reduction in competitor prices exceeding 15%. *Id.* at ¶ 11. Furthermore, U.S. consumers of telecommunications infrastructure would reap even more substantial benefits if Huawei were permitted to compete freely within the U.S. Non-U.S. markets have seen a discernible increase in competition where Huawei is able to compete freely. Equipment critical to mobile broadband access—such as Radio Access Network ("RAN") equipment and LTE base stations—is priced higher in North America than in any other region in the world. *Id.* This can be attributed to the fact that Huawei and ZTE have a much smaller presence in the U.S. as a result of political factors. *Id.* at ¶ 10. As next-generation technologies such as 5G are deployed across the world, prohibiting Huawei from providing equipment to the U.S. market could ultimately raise prices, reduce innovation, and limit the U.S. in keeping up with its global counterparts.

D. The Comments Confirm That Benefits Would Be Speculative and Minimal

Huawei showed that the proposed rule could not reasonably be projected to result in any significant public benefit in terms of improved network security or reliability, for several reasons. First, the lack of any criteria or process for identifying national security threats, and the Commission's lack of expertise and resources in that area, means the risk of false positives (blacklisting companies that do not actually pose a threat) and false negatives (failing to blacklist companies that do pose a threat) is high. Second, the proposal would do nothing to address threats to network security and reliability arising from sources other than the final seller of a product or service. Third, it would ban even equipment and services that, by their nature, are incapable of posing threats to national security. And, fourth, it fails to analyze the threat level associated with the purchaser of the product or services, thus banning purchases even by buyers who are extremely unlikely to be the target of a hypothetical network attack. *See* Huawei Comments 54-56.

Competitive Carriers Association agrees that the benefits of the proposed rule are unspecified and unquantifiable, and points out that the burden is on the Commission to demonstrate that its proposal will yield specific benefits that justify its costs. Competitive Carriers Association Comments 34. It also points out that, "even assuming the importance of securing the supply chain, the Commission has failed to tailor the rule to the danger at issue." *Id.* at 29. Similarly, NCTA—Internet & Television, while skeptical of unilateral Commission action in this area, suggests that "[a] cost-benefit analysis is crucial to achieving the goal of managing supply chain risks without undue economic harm and without unintended and unwanted consequences." NCTA—Internet & Television Comments 2. Sagebrush also comments that the significant costs that the proposed rule

would impose on it and its customers would not have "any corresponding benefits." Sagebrush Comments 2.

E. TIA's Analysis of Benefits is Logically Flawed and Factually Unfounded

TIA is the only commenter that attempts to expand upon the NPRM's minimal analysis of the potential benefits of the proposed rule, but it fails to demonstrate that the proposed rule provides the benefits that it claims. In particular, TIA asserts that the proposed rule yields "significant public interest benefits for all stakeholders" by promoting quality and equality of service; reducing costs of breaches and protection; and increasing consumer confidence. TIA Comments 67-71. However, not only does TIA provide no evidence in support of its assertion, but the record actually demonstrates that the proposed rule would likely *impede* American consumers from receiving these alleged benefits.

1. Quality of service

TIA argues that the proposed rule would improve the quality of communications services, consistent with the Commission's statutory directives. TIA Comments 67-68. But, predictably, TIA is unable to show that Huawei products have or would have a negative impact on the quality of U.S. telecommunications services. Indeed, Huawei equipment is designed, developed, and produced with the most current and stringent cybersecurity protocols. Dowding Reply Decl. ¶¶ 9-10. Adherence to those rigorous standards is evidenced by the number of carriers in the record who have chosen to utilize Huawei equipment after undertaking a due diligence investigation of product security precisely *because* Huawei products are reliable, secure, and high-quality. *See, e.g.*, Sagebrush Comments 2, 4; Twain Communications Comments 4; WTA—Rural Broadband Comments 4. Furthermore, TIA's argument is logically inconsistent with its assertion that Huawei's presence

in the U.S. market is not "significant." TIA Comments 71. If that is the case, then any quality improvement resulting from blacklisting Huawei would have to be very small as well.

TIA acknowledges (at 68) the statutory directive that "individuals and business benefiting from subsidies in rural areas should have access to services that are 'reasonably comparable' to services in urban areas." Huawei agrees, and further agrees that the Commission should endeavor to ensure quality communications services are available to American consumers. However, Huawei's presence in rural and remote areas of the U.S. contributes to the availability of "reasonably comparable" services in the first place. *See, e.g.*, Competitive Carriers Association Comments 23; WTA—Rural Broadband Comments 4. As such, by TIA's own standards, the proposed rule would actually harm the quality of communications services in the U.S.

2. Reduction of costs for cyberattacks and breaches

TIA further argues that the proposed rule would "go far toward sparing U.S. businesses the economic costs associated with breaches and online distributed threats," citing reports that malicious cyberactivity cost the U.S. economy between $57 billion and $109 billion in 2016. TIA Comments 69. But, in the same comments, TIA argues that the loss of Huawei and ZTE would have minimal impact on the competitive market because of their minute market share. *Id.* at 71. By this logic, excluding Huawei and ZTE from the U.S. marketplace would also have minimal impact on the cost of cyberattacks and breaches. And, in any event, TIA offers no evidence that any portion of the costs it cites have been attributable to vulnerabilities or other failings in equipment supplied by Huawei or other targeted companies.

In fact, TIA errs in asserting that the proposed rule would reduce the cost of cyberattacks and breaches *at all*. As TIA has noted previously, "product security is a function of how a product is made, used, and maintained, not by whom or where it is made." 2013 TIA Letter 1. Huawei's

longstanding commitment to cybersecurity and loyalty from U.S. carriers have consistently demonstrated that Huawei products are made, used, and maintained with product security as a priority. TIA may point to a hefty number to highlight the high cost of malicious cyberactivity, but it puts forth no evidence of where these costs arise, and certainly none that point to Huawei. Instead, TIA seeks to assign causation where not even correlation exists.

3. Consumer Confidence

Last, TIA argues that the proposed rule provides "intangible benefits" by "preserv[ing] confidence among consumers and the private sector generally." TIA Comments 69-70. TIA asserts that lack of consumer confidence could "ultimately harm broadband deployment, consumer adoption, and/or drive some rural consumers to incur additional costs." *Id.* at 69. But, as established above, excluding Huawei equipment from the U.S. marketplace would inhibit broadband deployment and deprive carriers in rural and remote areas of a cost-effective means for providing necessary services—discrete, tangible harms that the proposed rule would certainly cause. Conversely, the consumer confidence "benefit" that TIA alleges is merely the *appearance* of one, ultimately creating a false sense of security to the detriment of American consumers. This is consistent with the position that TIA has previously taken—in 2013, TIA advocated against a similar equipment ban, arguing that "[g]eographic-based restrictions on equipment run the risk of creating a false sense of security when it comes to advancing [U.S.] national cybersecurity interests." 2013 TIA Letter 1. Furthermore, there is no evidence that U.S. consumers are actually concerned about the alleged security threat posed by Huawei or how many U.S. consumers share the alleged concerns. Nor is there evidence demonstrating the economic impact of such concerns or to show that consumers' confidence resulting from the proposed rule will outweigh the costs incurred by the proposed rule.

V. EVEN IF THE COMMISSION HAD AUTHORITY TO EXCLUDE A COMPANY FROM SELLING EQUIPMENT, IT COULD NOT DO SO WITHOUT FIRST PROVIDING NOTICE AND A MEANINGFUL HEARING

Huawei's opening comments explain that the proposed rule denies blacklisted companies the process to which they are entitled under the Due Process Clause, the APA, and the Communications Act. Under the Due Process Clause, the Commission may not blacklist a company unless it first provides the company with notice and the opportunity for a meaningful individualized hearing on the charges against it, even if the Commission has the authority to create such a blacklist, which it does not. Under both the Due Process Clause and the Communications Act, this hearing must include a meaningful opportunity for the company to review and respond to the evidence against it. Further, under the APA, this hearing must constitute a formal adjudication that complies with the APA's rigorous "on the record" hearing requirements. Huawei Comments 59–86; *id.* Ex. H, Hammond Decl. 1–19.

Other commenters agree with Huawei that due process guarantees the right to review and respond to the evidence on which the blacklisting decision rests. Most notably, the Competitive Carriers Association agrees that "the Commission's proposed rule will violate … due process rights" because it "fails to provide an opportunity to review the unclassified evidence on which the official actor relied" and because it denies "stakeholders … a real opportunity to rebut [that] evidence." Competitive Carriers Association Comments 41–42. The Competitive Carriers Association explains that "[f]ailing to present directly affected entities with the evidence relied upon by the Commission will infringe the due process rights of those affected entities." *Id.* at 42.

Moreover, more than a dozen commenters—including even supporters of the proposed rule—have reinforced Huawei's argument that the Commission's proposed rule that blacklists

companies would violate the APA by producing unreasonable secondary retroactivity. Huawei Comments 80–81. For example, the Rural Broadband Alliance notes that "tearing out" existing networks is "an enormous physical and economic challenge," "heretofore unthinkable," "an existential threat to the entire business," and "potentially catastrophic." Rural Broadband Alliance Comments 14. Competitive Carriers Association likewise points out that the proposed rule would require carriers "to rip up and replace" "existing equipment" under "existing contracts." Competitive Carriers Association Comments 46. Rise Broadband emphasizes that the "costs" of "revamping ongoing USF-supported network construction" and "replacing 'banned' equipment" "would be patently unreasonable." Rise Broadband Comments 7. Twain Communications explains that "the costs associated with the replacement of existing equipment … impos[e] a significant and unreasonable financial burden on rural telecommunications companies." Rise Broadband Comments 3–4. Pine Belt Cellular agrees that "the costs associated with the replacement of existing network equipment" banned by the proposed rule are "significant and unreasonable." Pine Belt Cellular Comments 5. And so on. *Accord* NCTA—Internet & Television Comments 15; NTCA—Rural Broadband Comments 24; Puerto Rico Telephone Comments 7; American Library Association Comments 3; TracFone Comments 6; USTelecom Comments 15; WTA—Rural Broadband Comments 15. The Commission cannot avoid these problems simply by grandfathering past equipment purchases; the lack of interoperability between old equipment made by one manufacturer and new equipment made by another would mean that, as a practical matter, even past purchases will inevitably be affected. *See* Section IV.B.2 above.

Only a single supporter of the proposed rule, TIA, specifically addresses the procedural issues raised by the Commission's proposal. Even TIA, however, *agrees* with Huawei on a number of points. For example, TIA acknowledges that the Commission "should afford targeted companies

some measure of due process." TIA Comments 81. TIA adds that "such due process may also be legally required" and that, under "D.C. Circuit" precedent, due process guarantees notice, "the right to receive any non-classified evidence," and "the right to challenge [the] determination." *Id.* at 82. So too, TIA agrees that "the Commission should not insert company names into the Code of Federal Regulations," that "any action by a regulatory agency to restrict a single company by name in a rule is an extremely rare practice," and that "the Commission should not go down this path." *Id.* at 60–62. As Huawei has already explained, such an approach would violate the due-process prohibition on using rulemaking to deprive a small group of people of liberty, contravene the Bill of Attainder Clause by targeting a small group of people for punitive measures, and violate the APA by producing unreasonable secondary retroactivity. Huawei Comments 76–81.

That said, TIA's specific proposals fall short of the process required by the Constitution and statute. To start, TIA's proposed rule text includes no procedural protections at all—no notice, no hearing, no opportunity to review evidence, and no opportunity to respond to evidence. TIA Comments, App. The proposed rule text thus fails to provide even the minimal procedures that TIA's own comment acknowledges are required.

TIA proposes the creation of an "interagency process that is empowered to make national security determinations on behalf of the entire … federal government." *Id.* at 80. TIA adds, however, that "such a process could be established by statute [or] executive order"; it does not claim that it could be established by the Commission's regulations. *Id.* Rightly so. For one thing, it should go without saying that the Commission lacks the power to establish processes "to make national security determinations on behalf of the entire federal government." *Id.* For another thing, Huawei's initial comment explains why the Communications Act does not grant the Commission the authority to rest USF decisions on purported national-security concerns. And, in any event, the

presumption against subdelegation would preclude the Commission from handing off any such authority to some other entity, such as TIA's proposed "interagency" body. Huawei Comments 81.

TIA further proposes that any blacklist should cover companies that Congress, the President, or an interagency body designate as national-security threats. TIA Comments 55. Others suggest that the Commission should rely on designations made through a supply chain risk assessment being undertaken by the Department of Homeland Security. USTelecom Comments 8-14. For the reasons Huawei has already identified, however, any such approach would be unlawful: The Due Process Clause does not allow the Commission to treat an existing statute, order, or designation as a substitute for a meaningful hearing. Huawei Comments 82, 84. In addition, piggybacking on existing statutes, orders, and designations would be arbitrary and capricious, because the context surrounding the earlier action may differ sharply from the context surrounding the later blacklisting. For example, it would be arbitrary and capricious to conclude that, just because Congress prohibited a particular company from supplying equipment to ballistic-missile facilities in the 2018 NDAA, the Commission should prohibit the company from supplying equipment to rural libraries. *Id.* at 83.

Finally, TIA proposes that one criterion for blacklisting a company is whether the company has been subjected to "government investigations" into whether it "has engaged in illegal activity." TIA Comments 83. In other words, in TIA's view, a mere *investigation* into alleged unlawful activity could trigger blacklisting, regardless of whether any unlawful activity is ultimately proven. It is difficult to imagine a more direct assault on the procedural principles underlying the American system of justice. "The principle that there is a presumption of innocence in favor of the accused is the undoubted law, axiomatic and elementary, and its enforcement lies at the foundation of the

administration of our criminal law." *Coffin v. United States*, 156 U.S. 432, 453 (1895). To treat a mere investigation as a badge of guilt is to contradict this "axiomatic," "elementary," and "undoubted" legal rule.

At bottom, "due process is 'the protection of the individual against arbitrary action.'" Huawei Comments Ex. H, Hammond Decl. 18 (quoting *Ohio Bell Tel. Co.* v. *Pub. Utils. Comm'n of Ohio*, 301 U.S. 292, 302 (1937)). As Huawei's Comments established, "[u]sing a rulemaking proceeding to blacklist entities" in the manner the Commission proposes "harkens back" to "[m]any of our country's darkest moments," which have been "marked by exercises of legislative and executive power against individuals without due process of law." *Id.*; *see also* Huawei Comments 59–86. The comments submitted by other entities do nothing to undermine—and, in fact, forcefully underscore—this critical point.

VI. THE PROPOSED RULE RELIES ON UNSUPPORTABLE FACTUAL ALLEGATIONS AGAINST HUAWEI

Fundamentally, a security vulnerability must be identified before it can be fixed. Huawei's Comment shows that the proposed rule is largely motivated by unverified, unproven, and unspecified allegations against Huawei and a handful of other companies. Huawei Comments 86–91. A multitude of other commenters agree.

For example, the Competitive Carriers Association comments that the Commission has identified "no specific evidence that Huawei or ZTE equipment and services create cybersecurity risk." Competitive Carriers Association Comments 39. The head of Viaero has submitted a declaration that Viaero buys equipment and services from Huawei, yet remains protected "from any malicious act." *Id.*, DiRico Decl. ¶ 3. The CEO of United has likewise submitted a declaration that,

even though "nobody wants to protect our National Security more than United," United feels comfortable using "Huawei equipment." *Id.*, Houseman Decl. ¶ 6. NTCA—Rural Broadband adds that "border patrol agents … roam freely between U.S. network providers and those operated by neighboring countries which often rely upon Huawei equipment"—all without raising any apparent security concerns. NTCA—Rural Broadband Comments 16. Twain Communications, which uses "equipment manufactured by Huawei," has not seen any evidence" that the blacklisting of the company is "even reasonably related … [to] the goal of national security." Twain Communications Comments 3–4; *accord* Pine Belt Cellular Comments 5. And Sagebrush "has spent extensive time trying to find one shred of evidence that demonstrates any wrongdoing by Huawei and, to date, has been unable to uncover any hard fact." Sagebrush Comments 4.

TIA paints a different picture, but its analysis is fundamentally flawed. TIA asserts that "various government entities have raised concerns regarding Huawei." TIA Comments 11; *see id.* at 14–18. Every single example that TIA identifies, however, either cites no evidence or relies ultimately on the 2012 Report of the House Permanent Select Committee on Intelligence ("2012 HPSCI Report"). *Compare, e.g.*, TIA Comments 16 (citing H.R. 5515), *with* H.R. 5515 § 880 (citing 2012 HPSCI Report). Indeed, the governments of many countries, including the United Kingdom, Canada, and Finland have expressed their confidence in Huawei's equipment. As a spokesman for the UK's National Cyber Security Centre explained, for instance, "Huawei is a globally important company whose presence in the UK reflects our reputation as a global hub for technology, innovation and design. This government and British telecoms operators work with Huawei at home and abroad to ensure the UK can continue to benefit from new technology while

managing cyber security risks." [29] And in Canada, Public Safety Minister Ralph Goodale, insisting that measures were in place to protect Canadians from possible foreign espionage, told Parliament that the government would not block Huawei from doing business in Canada. [30] Corroborating that report, Bruce Rodin, vice president of wireless networks for Bell Canada, stated that during the ten years his company had used a cyber-security firm to extensively test Huawei products, his company has "never seen malicious code or backdoors."[31] The moves underway in the United States, Rodin explained, are "a commercial thing. They are protecting their industry."[32] Similarly, Deutsche Telekom, which works collaboratively with Huawei, has explained that "[t]he hardware is built to Deutsche Telekom's specifications and is examined by our own security department."[33]

If any U.S. (or other) government entity were aware of a deliberately compromised product manufactured by Huawei, it undoubtedly would have immediately notified Huawei and put substantial pressure on Huawei to resolve the compromise. Furthermore, it would have warned Huawei's existing customers to remove the identified product(s) and/or not to buy specific Huawei products in the future. However, the U.S. government has not raised a single concern to Huawei or its customers regarding such allegedly compromised products nor has it requested a forensic

---

[29] Jay Jay, *Despite U.S. ban, Huawei still enjoys much love from UK's NCSC*, TEISS (Feb. 21, 2018), https://teiss.co.uk/information-security/huawei-uk-ncsc-cyber-security/.

[30] Robert Fife & Steven Chase, *Federal government won't block Huawei's business in Canada*, The Globe and Mail (Mar. 19, 2018), https://www.theglobeandmail.com/politics/article-federal-government-wont-block-huaweis-business-in-canada/.

[31] Eric Auchard & Sijia Jiang, *China's Huawei set to lead global charge to 5G networks*, Reuters (Feb. 23, 2018), https://www.reuters.com/article/us-telecoms-5g-china/chinas-huawei-set-to-lead-global-charge-to-5g-networks-idUSKCN1G70MV.

[32] *Id.*

[33] *Id.*

examination of any Huawei products in the context of security vulnerabilities. *See* Dowding Reply Decl. ¶ 13. The fact that the U.S. government—or any other government, for that matter—has not raised specific concerns leads to the only possible conclusion: No one has ever found that Huawei offered a deliberately compromised product.

Huawei has already explained why reliance on the 2012 HPSCI Report is misguided, and no commenter has refuted its analysis. The Report lacks detail and identifies no specific evidence that Huawei poses a threat to national security. Instead, the Report rests on the erroneous premise that "it appears that under Chinese law, ZTE and Huawei would be obligated to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security." 2012 HPSCI Report 3. Huawei has shown that this premise is wrong. No Chinese law requires a company such as Huawei, much less an overseas subsidiary such as Huawei Technologies USA, to cooperate with the Chinese Government in this way. Huawei Comments 43; *id.*, Ex. D, Ye Decl. ¶¶ 9–15; *id.*, Ex. E, Chen & Fang Decl. ¶¶ 84–85.

It is thus no surprise that other commenters agree that the Commission would be acting arbitrarily and capriciously by relying on the 2012 HPSCI Report (or on sources that, in turn, rely on the Report). According to the Competitive Carriers Association, "[the] 2012 House Committee report [is] a very thin justification for a rule that threatens to upend an industry," particularly because the report "itself lacks any detail on the risks posed by the targeted companies." Competitive Carriers Association Comments 4, 34. And according to Computers & Communications, "the report does not offer specific information on security threats." Computers & Communications Comments 2. These criticisms are on the mark.

VII. THE COMMENTS SUPPORTING THE PROPOSED RULE ARE OTHERWISE UNPERSUASIVE

Commenters' remaining proposals in favor of the Commission's proposed rule are problematic. Each should be rejected.

Nokia, in an ex parte letter, urges the Commission to use "a totality-of-the-circumstances approach" to determine whether "a company is a trusted vendor." Nokia Letter 2. But using that approach here would be arbitrary and capricious. The Communications Act's enumerated universal-service principles include a directive to adopt "specific, predictable and sufficient Federal and State mechanisms to preserve and advance universal service." 47 U.S.C. § 254(b)(5). A totality-of-the-circumstances test contradicts this demand for specificity and predictability. As the Supreme Court has explained, "[a] totality-of-the-circumstances test … is really, of course, not a test at all but an invitation to make an ad hoc judgment." *City of Arlington* v. *FCC*, 569 U.S. 290, 307 (2013). Any such "test" tends to lead to "unpredictable" and even "chao[tic]" outcomes. *Id.* Concretely, it would make it difficult for carriers and equipment manufacturers to make decisions about investments and contracts, because the test would leave them uncertain about which companies the Commission will blacklist in the future. Indeed, even Nokia acknowledges that "[un]predictable criteria" can lead to "market uncertainty." Nokia Letter 2. Regardless of whether such uncertainty is tolerable in other areas of administrative law, it is intolerable here, where Congress has put a special premium on "specific[ity]" and "predictab[ility]." 47 U.S.C. § 254(b)(5).

More specifically, Nokia urges the Commission to "consider the existence of [a national-security agreement], or other comprehensive supply chain focused agreement between the U.S. and a supplier as one indicator of a supplier's trustworthiness and suitability." Nokia Letter

2–3. But this would not be a sensible criterion. First, companies typically enter into national-security agreements in the context of particular transactions, license applications, or investigations; to Huawei's knowledge, no company has ever been asked by the Government to enter into such an agreement outside the context of a particular transaction. It is arbitrary to infer that, just because a particular company happens to have engaged in a transaction that calls for a national-security agreement, it is somehow more trustworthy than a company that has not engaged in such a transaction. Second, if the existence of a national-security agreement is to be made a criterion, then every company must be given the opportunity to enter into such an agreement. Yet none of the Commission, relevant agencies, CFIUS or Team Telecom has ever offered such an opportunity to Huawei. Finally, Nokia never identifies the particular terms that such agreements would need to contain. If the Commission agrees that a national-security agreement can resolve a supposed threat to national security, the Commission should (as Huawei has argued) explain what terms it requires in such agreements, so that Huawei and others can evaluate them and have the opportunity to enter into such an agreement. Huawei Comments 41. After all, the statute demands specificity and predictability, *see* § 254(b)(5), which are surely not satisfied by a vague reference to an unspecified national-security agreement.

Nokia also proposes that the Commission consider other factors, such as whether a company is publicly traded on one or more exchanges, whether the company is a CTPAT (Customs-Trade Partnership Against Terrorism)-verified provider, and whether a company has a history of complying with U.S. laws and regulations, including laws and regulations pertaining to sanctions and export controls. *See* Nokia Letter at 2-3. But Nokia never explains why the factors it urges the Commission to consider are relevant or do not result in double-counting. For example, ZTE is a

public company, so it is unclear how Nokia would weigh this factor in a decision whether to black-list ZTE. Further, if a company is CTPAT-verified (because it "agree[d] to voluntarily participate" and "conducted a risk assessment" such that it is "considered to be of low risk"[34])—as Huawei is—why does it make sense to ask if the company is publicly traded? Surely financial disclosure requirements shed no light on whether a company is working with a foreign government to compromise the United States' national security—in contrast to a program like CTAPT, which asks questions that are actually relevant to border security. The same goes for a prior history of compliance with U.S. law and regulations, which, by itself, says little about a company's susceptibility to foreign government influence.[35] Just as with national-security agreements, if the U.S. government has questions about a supplier's activities, it should simply ask relevant questions or require relevant certifications or assurances. Nokia's laundry list of "factors" of unclear weight would allow decisionmakers to pick and choose those factors that happen to tilt in the direction of a preferred outcome, and ignore those that do not.

For its part, Motorola Solutions, Inc., argues (Comments 5-7) that the FCC's prohibition should be extended to public-safety communications networks. As an initial matter, as the comments of AT&T correctly explain (at 4), and as Huawei explains above, the NPRM identifies no

---

[34] U.S. Customs & Border Prot., *CTPAT: Customs Trade Partnership Against Terrorism*, https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat (visited June 25, 2018).

[35] If sanctions violations were deemed relevant to determining whether a company poses a threat to national security, the Commission would have to review the settlement Ericsson reached earlier this year with the Department of Treasury regarding an alleged conspiracy between Ericsson employees and a Lebanese company to violate the Sudanese Sanctions Regulations. *See* Settlement Agreement, May 3, 2018, available at: https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20180606_ericsson_settlement.pdf. However, Huawei submits that these types of issues are actually irrelevant to a rational determination of national-security threats.

authority that would allow the FCC to expand its proposal beyond the USF context. In any event, even if it were legally proper and reasonable for the FCC to impose its rule on public-safety communications networks—a move that would have significant effects and is far afield from the USF context on which the current NPRM focuses—the FCC would, at a minimum, need to issue a Further Notice of Proposed Rulemaking and afford interested parties an opportunity to comment. If the FCC were to expand its current proposal to the context of public-safety communications networks without issuing a further NPRM, it would violate the APA's logical-outgrowth rule. *See, e.g.*, *Envtl. Integrity Project* v. *EPA*, 425 F.3d 992, 996-98 (D.C. Cir. 2005).

TracFone proposes that the Commission clarify that the proposed rule is "strictly limited to network management equipment and infrastructure" that directly relate to network management. TracFone Comments 2. TracFone argues that a more narrowly tailored rule applicable only to facilities-based providers and network management equipment would achieve the Commission's goals in this proceeding. *Id.* at 5-6. TracFone proposes that existing end-user devices used in conjunction with the Lifeline program should be grandfathered. *Id.* at 6. However, a rule applicable only to equipment used for network management would not avoid the substantial costs of the proposed rule to rural carriers and ultimately consumers, including in particular those low-income consumers served by rural carriers.

VIII. CONCLUSION

For the foregoing reasons and those in Huawei's initial comments, the Commission should not adopt the proposed rule, and should terminate this rulemaking proceeding. Adoption of the proposed rule would be contrary to the Constitution, would exceed the Commission's jurisdiction under the Communications Act, would be arbitrary and capricious, and would violate the procedural requirements of both the Communications Act and the APA.

Respectfully submitted,

Andrew D. Lipman
Russell M. Blau
David B. Salmons
Catherine Kuersten
Patricia Cave

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave, NW
Washington, DC 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
david.salmons@morganlewis.com
catherine.kuersten@morganlewis.com
patricia.cave@morganlewis.com

Counsel to Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc.

Glen D. Nager
Bruce A. Olcott
Ryan J. Watson
Vivek Suri
Parker Rider-Longmaid

JONES DAY
51 Louisiana Ave, NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)
gdnager@jonesday.com
bolcott@jonesday.com
rwatson@jonesday.com
vsuri@jonesday.com
priderlongmaid@jonesday.com

LIST OF EXHIBITS

Exhibit A	Reply Declaration of Donald Purdy, Jr.
Exhibit B	Letter to Representatives J. Boehner, H. Reid, N. Pelosi, and M. McConnell (April 4, 2013)
Exhibit C	Reply Declaration of Thomas Dowding
Exhibit D	Reply Declaration of Allan L. Shampine

EXHIBIT A

REPLY DECLARATION OF DONALD A. PURDY, JR.

I, Donald A. Purdy, Jr., hereby declare, affirm, and state the following:

I. Introduction

1. The facts set forth below are known to me personally, and I have firsthand knowledge of them.

2. I make this declaration in support of reply comments submitted by Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc. ("Huawei") in response to a Notice of Proposed Rulemaking ("NPRM") promulgated by the Federal Communications Commission ("FCC"), In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, FCC 18-42, on April 18, 2018.

3. I hereby incorporate by reference my prior Declaration, submitted as Exhibit B to the Comments of Huawei, filed on June 1, 2018 in Docket No. 18-89.

4. In this affidavit, I will discuss the global supply chain for information and communications technologies, cyber security risk, supply chain risk management, and the implications for cyber defense from another angle. In response to various submissions to the FCC concerning standards, certification processes, and best practices on supply chain security management, I also will elaborate on Huawei's views and practices.

5. As my colleague John Suffolk and I explained in our initial Declarations, Exhibits A and B to the Huawei Comments, respectively, as well as in Huawei's Cybersecurity

whitepapers,[1] the supply chain for telecom equipment is global and highly complex. Any piece of equipment will contain components and software from multiple companies and countries.

6. The "name on the box" reveals very limited information about the nature and origin of the equipment, and barring equipment based on that name would be arbitrary and would not materially improve security. In reality, networks and systems around the world, and their supply chains, are vulnerable to cyber attacks from sophisticated and unsophisticated malicious actors – including nation states – that frequently use unsophisticated attack methods. This is true regardless of who makes the equipment in those networks and systems. The recent OMB report on federal agencies' use of the National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("CSF") shows that even a government as well-intentioned and motivated as the U.S. about cybersecurity risks in general, and supply chain risk in particular, has difficulty implementing measures to appropriately address cybersecurity risk. The key way for the FCC to help improve the cybersecurity of telecom networks is to identify policies that will increase adoption of such risk-based measures throughout the telecommunications industry, not to arbitrarily bar products from a handful of manufacturers.

7. A realistic analysis of telecom carrier risks associated with supply chains leads me to conclude that the proposed FCC solution ignores a much broader set of concerns regarding the vulnerable, global telecommunications supply chain; does not improve the security of targeted infrastructures; and fails even to address fully the primary concern

---

[1] I was the primary author of Huawei's June 2016 white paper titled "The Global Cyber Security Challenge – It is time for real progress in addressing supply chain risks," which provides more details on supply chain risk management. Exhibit I to the Comments of Huawei, filed on June 1, 2018 in Docket No. 18-89.

that led to this proposal, namely, potential Chinese or other nation-state entities leveraging or exploiting telecom vendors and products for malicious purposes. In the end, the exclusion of any individual vendor or set of vendors, based in whole or in part on the location of their headquarters, from participating in carrier-contracted activities, would have a negligible effect on telecom infrastructure security.

II. Cybersecurity Risk

8. There is widespread consensus that it is not possible to eliminate all cybersecurity risk and that a risk-based approach is necessary to assess and address cybersecurity risk, consistent with an organization's risk posture and objectives.

9. The NIST CSF is an increasingly well-recognized tool for assessing and addressing cybersecurity risk, and was recently amended to call for organizations to apply recognized supply chain risk management ("SCRM") processes to their suppliers of products and services and to appropriately consider supply chain risk as part of the organization's overall risk posture.

10. The recently released Department of Homeland Security ("DHS") cyber strategy similarly emphasizes the importance of comprehensive risk management for organizations, industry sectors, government operations and services, and the cyber security risk of a nation.

11. The FCC Advisory Group, the Communications Security, Reliability and Interoperability Council ("CSRIC"), with the support of the FCC, has made available guidance for the use of the NIST CSF for the participant-organizations in the telecommunications sector (2015, *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report*), including guidance related to supply chain risk (2016, CSRIC V, *Secure*

Hardware and Software: Security-By-Design Working Group 6: Final Report (March 2016); and CSRIC V, *Secure Hardware and Software: Security-By-Design Working Group 6: Final Report* (September 2016)).

12. Experts agree that a risk-based assessment is necessary to determine what risk-mitigation measures are appropriate. For example, only the most critical, highest-risk systems and networks require the most sophisticated risk-mitigation measures, such as the use of trusted foundries to manufacture/assemble key components. *See*, for example, the Defense Science Board Task Force Report on Cyber Supply Chain (February 2017, DTIC # AD1028953, https://www.acq.osd.mil/dsb/reports/2010s/1028953.pdf) and NDIA Trusted Microelectronics Joint Working Group (2017, http://www.ndia.org/divisions/working-groups/tmejwg/final-team-reports).

III. Supply Chain Risk Management

13. This same risk management approach should be applied to the supply chain for the U.S. communications sector.

14. NIST provides a number of important references and guides including, for example: (1) The NIST CSF, as amended to explicitly reference supply chain risk (Framework V1.1 (PDF); (2) Introduction to the Components of the Framework (Framework V1.1) ICT SCRM tools and metrics, and mitigation strategies and methodologies (https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/nist_ict-scrm_fact-sheet.pdf); (3) a NIST Cybersecurity Framework Reference Tool (NIST Cybersecurity Framework (CSF) Reference Tool); (4) NIST Cybersecurity Framework - Industry Resources; (5) NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and

Organizations; and (6) draft NIST IR 8170 (The Cybersecurity Framework: Implementation Guidance for Federal Agencies). NIST likewise recommends that "Federal agencies manage information and information systems according to the *Federal Information Security Management Act of 2002* ("FISMA") and a suite of related standards and guidelines. Perhaps the most central FISMA-related publication focused on risk managment is NIST Special Publication (SP) 800-37 – *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, which details the Risk Management Framework ("RMF"). The RMF six-step process provides a method of coordinating the inter-related FISMA standards and guidelines to ensure systems are provisioned, assessed, and managed with appropriate security.

15. The record in this proceeding, in addition to discussion of the NIST CSF and CSRIC recommendations, includes other submissions that recommend and discuss how to apply cyber risk management principles to the communications supply chain. See, e.g., Rural Broadband Alliance Comment, Ex. 1.

16. From my point of view as a security professional – without necessarily endorsing the particulars of any of them – these types of risk-based approaches have various clear advantages relative to what the FCC has proposed.

17. For example, they assess and address risks, systematically, across a range of threat vectors regardless of whether the threat originates in the software or any particular component and regardless of where the software/component was made.

18. It is important to address the full range of risk components – threat, vulnerabilities, and consequences. It doesn't make sense to address only isolated, even speculative risks,

without addressing risk comprehensively. Any serious attempt to address supply chain risk should consider options for doing so in a comprehensive manner, not the approach that the FCC has proposed, which is not even ostensibly comprehensive.

19. Some supporters of the FCC proposal claim that risk-based measures such as testing are intended only for unintentional vulnerabilities and are incapable of detecting intentional vulnerabilities. This fails to recognize the current capabilities of testing professionals and real-world experience with testing, which demonstrate that a well-designed testing program is capable of finding intentional vulnerabilities as well as unintentional ones. Of course, no single testing regime will be perfect and detect all vulnerabilities. But at a minimum, independent testing should be part of the arsenal available to make sure that vendors are meeting their obligations regarding self-testing, disclosure, and remediation.

IV. Huawei's Exemplary Practice in Supply Chain Risk Management[2]

20. The ICT industry has developed standards, certification requirements, and best practices to ensure that their communication products work as expected without compromising communication. Those standards and certification requirements contain not only technical specifications, but also the processes and procedures to develop, build, and maintain secure products.

21. These standards, certification requirements, and best practices ensure that a product fulfills the intended characteristics and was built in accordance with them. They reduce the risk of vulnerabilities and malicious hardware and software but they cannot by themselves prove that a product is free of vulnerabilities or malicious software or hardware. To help resolve this gap, Huawei has made additional efforts to answer three fundamental questions:

1) Is the product supply chain to the customer sufficiently secure (including updates)?

[2] For the purposes of this declaration, I do not exhaustively enumerate all of Huawei's efforts in supply chain risk management. More information can be obtained in Huawei's cyber security white papers and other documents.

2) Is the product built without intentional malicious software or hardware?
3) Has the product been adequately tested for vulnerabilities?

22. Regarding the first question - with trusted computing technology such as Huawei's Trusted Platform Module, or TPM, there is strong assurance that in Huawei's supply chain only the tested and intended software version is running on the customer's machine or device. In addition, Huawei has also made available a second, independent verification path (two roots of trust) to give the customer the fullest possible knowledge about the software running on its machine or device.

23. Regarding the question of how to verify that the software does not contain intentional malicious code, the foundation is industry standards and best practices for the build and release of software, as well as those that protect software against unwanted, malicious code, in general. This is partially expressed in the CSRIC V Working Group 6 best practices – security by design - which Huawei is following, including:[3]

(1) The software has to implement or support protection mechanisms against malicious code, like address randomization and separation technologies.

(2) The development and production process has to implement industry best practices to avoid a situation in which a single person or group of persons has access to the source code or production process and can tamper with it. Therefore, Huawei has implemented a segregation of duties, not only on an individual level, but also on an organizational level.

[3] TIA contends that banning the targeted companies *can be viewed as a top-level "identification" of risk*, based on the CSRIC V Working Group 6 best practices. It cannot. Nowhere in the CSRIC V Working Group 6 best practices is there an indication that banning a company could be a solution for national security. In fact, one of the targeted companies, ZTE, was a participant of the working group. 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, at 7 (Mar. 2016), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_FINAL_%20wAppendix_0316.pdf.

(3) In addition, as discussed in more detail below, the software and software production process is inspected by customers and government organizations and is tested using white-box and black-box testing methods.

24. To answer the third question on adequate testing, Huawei internally enforces industry standards and best practices in its processes, obtains security certifications according to these standards, and allows independent security experts to test its products, review source code, and inspect development and production processes. This is part of the white-box testing intended to minimize the risk of malicious components being inserted into the products, and significantly reduces the risk of such malicious components or code, and reduces the frequency and seriousness of vulnerabilities.

25. Further, local governments and Huawei customers routinely inspect and analyze the traffic in their networks that contain Huawei's equipment. Any traffic coming from suspicious sources or going to suspicious destinations will be identified and analyzed – thus reducing the possibility that there is a hidden communication channel for a product manufacturer in a carrier's or enterprise's network. In this respect, all Huawei products are constantly undergoing the most intensive black-box testing given Huawei's leading global market share, in addition to regular lab tests.

26. In summary:

1) Huawei's development, product and supply chain processes comply with ***industry standards and best practices***. That is the foundation for secure products.
2) Huawei provides customers with visibility into our product development and production processes as part of our ***white-box testing***.
3) Because today all network traffic is and should be monitored, any malicious traffic from or to a machine or device should be identified. That is, in effect, a ***continuous black-box test***.

V. Barring Huawei On the Ground That It Presents a National Security Threat is not Warranted

27. A company should not be barred as a national security threat if it is compliant with industry best practices and standards; its products are accessible for external assessments by independent third parties and various government regulators; and its products are effectively subject to continuous white-box and black-box testing.

28. In addition, hidden functionality and intentional vulnerabilities are always at risk of being discovered – particularly as time passes -- and inevitable widespread publication of any such discovery would have a tremendously negative impact on the vendor. That alone represents a major deterrent to improper conduct. Given the ability of sophisticated malicious actors – including nation states – to exploit other widely available vulnerabilities using less sophisticated (and less attributable) means, it makes no sense for a vendor or even a suspect government to risk damage to the vendor by intentionally implanting malicious functionality into a product or component that is likely to be discovered at some point.

29. Huawei's products and source code are regularly provided to external security experts for testing and certification, and Huawei products are exposed to customers and hackers around the world. If there were any backdoor, deliberately implanted or not, it would be discovered sooner or later. However, so far, the industry has not found Huawei's products to include a backdoor.

30. Our customers throughout the world trust Huawei. Huawei will never do anything that undermines that trust, which could put Huawei's entire business at jeopardy, and threaten the livelihood of over 170,000 employees. On the other hand, the incremental advantage to a malevolent adversary of manipulating Huawei to implant a backdoor is extremely

limited, compared to the readily available opportunity to exploit the target-rich environment that is the modern ICT supply chain and the vulnerable networks and systems of ICT owners and operator in the global market.[4]

31. This is illustrated by the theoretical examples set out in the TIA Comments of hard-to-find, deliberate vulnerabilities. TIA Comments at 36-38. Those examples enable malicious activity according to a certain time schedule or only in response to a specified sequence of events. A malicious actor could not know what data would be intercepted, let alone what value such data would have, through such a theoretical backdoor.

VI. What are the implications for cyber defense of the prevalence of cyber vulnerabilities and attack methods that can compromise just about any connected network or system?

32. Supporters of the FCC approach are wrong to suggest that blocking a few select companies will have any discernible impact on national security threats. Rather, a comprehensive cyber security risk management program that requires meaningful supply chain risk management processes to evaluate and mitigate risks from suppliers is necessary.

33. Risk-informed ICT Procurement Requirements should be developed and used by buyers of ICT products and services that are appropriate to mitigate risk, customized by sector or sub-sector, and/or risk environment. Such requirements, if widely used, will incentivize all vendors to improve the cyber hygiene and assurance of their products and components.

---

[4] Spiegel, Catalog Advertises NSA Toolbox, http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html, accessed June 27, 2018.

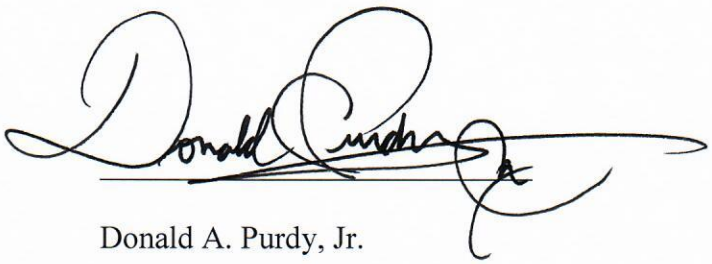
34. ICT purchasers should require vendors to test for known vulnerabilities, and share test results with customers, commit by contractual provision(s) to find and remediate the most significant vulnerabilities (*e.g.*, CVSS 7 and above) before deployment to customers, and remediate similarly significant, later-discovered vulnerabilities in a timely fashion.

35. If appropriate to the risk, as has been required – at least in part -- of vendors for the DHS Continuous Diagnostic and Monitoring ("CDM") program for federal agencies, ICT purchasers can require self-testing, disclosure, and remediation of known vulnerabilities (as recommended in paragraph 34); submission of a Bill of Materials for all products/components; and a binding statement by the vendor that they have applied recognized supply chain risk management processes to evaluate the risk from their suppliers of products and services, and appropriately mitigated the risk that the suppliers for whatever reason cannot mitigate.

36. For higher risk networks and systems (short of the most critical and highest risk systems), purchasers can require that independent testing programs be implemented to evaluate hardware and software and ensure that only tested components are deployed by customers. A well-designed testing program is capable of finding most vulnerabilities and hidden functionality. For the most critical, highest risk situations, a trusted foundry can be used to manufacture key components. *See*, for example, the Defense Science Board Task Force Report on Cyber Supply Chain (February 2017, DTIC # AD1028953, https://www.acq.osd.mil/dsb/reports/2010s/1028953.pdf) and NDIA Trusted Microelectronics Joint Working Group (2017, http://www.ndia.org/divisions/working-groups/tmejwg/final-team-reports).

I declare under penalty of perjury that the foregoing is true and correct.

Executed on July 2, 2018.



Donald A. Purdy, Jr.

DECLARATION OF DONALD A. PURDY, JR. EXHIBIT 1

DONALD A. (ANDY) PURDY, JR., J.D., CISSP, CIPP/US

8201 Kenfield Court *Andy.Purdy@comcast.net* *• 202/289-4019 -* **o**
Bethesda, MD 20817 *• 202/486-0720 -* **c**

OBJECTIVE: **IDENTIFY BOARD AND ADVISORY BOARD OPPORTUNTIES TO STRENGTHEN CYBER SECURITY AND PRIVACY RISK MANAGEMENT, INTERNAL GOVERNANCE, AND COMPLIANCE. POTENTIAL CYBERSECURITY AND PRIVACY ASSET FOR A CORPORATE RISK COMMITTEE.**

TO LEVERAGE A UNIQUE COMBINATION OF LEGAL AND CSO EXPERIENCE, AS A FEDERAL PROSECUTOR AND CONGRESSIONAL COUNSEL, AND AS ACTING GENERAL COUNSEL WITH THE U.S. SENTENCING COMMISSION, WORKING WITH THE U.S. ORGANIZATIONAL SENTENCING GUIDELINES AND CORPORATE COMPLIANCE PROGRAM REQUIREMENTS, AND AS A CORPORATE CSO EXPERIENCED WITH CYBERSECURITY AND PRIVACY RISK MANAGEMENT AND INTERNAL GOVERNANCE.

HIGHLIGHTS

- First CSO for Huawei Technologies USA; cybersecurity and privacy certifications.
- Advisor to emerging technology companies, including two that were acquired (BigFix by IBM and Lancope by Cisco).
- Chief Cybersecurity Strategist for CSC.
- Lead cybersecurity official for the U.S. government at DHS;
- White House role in helping to draft the *National Strategy to Secure Cyberspace*;
- Helped to formulate the Federal Sentencing Guidelines for organizations and individuals;
- Rich, diverse experience as a member of the national media and staffer on Capitol Hill; and
- Persuaded an initially incredulous congressional committee that the inescapable validity of the "single-bullet theory" proved that a single gunman killed President John F. Kennedy.

EXPERIENCE

Chief Security Officer (July 2012 to Present)
Huawei Technologies USA

Oversees Huawei USA's cyber security assurance and privacy strategy and program, and supports Huawei's global security assurance program. Chairs the Huawei USA Cyber Security and Privacy Committee.

Also the Huawei global lead for the East-West Institute Global Cooperation in Cyberspace Initiative and serves as the Vice Chair of the Open Group Trusted Technology Forum, which developed the Open Group Trusted Technology Provider Standard (O-TTPS), recognized by ISO as ISO/IEC 20243.

Chief Cybersecurity Strategist (February 2010 to June 2012)
CSC (Computer Sciences Corporation)

Provided strategic input to the development and implementation of a coordinated, company-wide initiative to address the cybersecurity needs of CSC's global client base, and worked in national and international venues to influence cyber security public policy and awareness.

Advisor to Emerging Companies (November 2006 to January 2010)
BigFix, Lancope, 3VR, HB Gary, Trust Defender

Acting Director and Privacy Officer (April 2003 to October 2006)[a]
National Cyber Security Division (NCSD)/
U.S. Computer Emergency Readiness Team (US-CERT)
Department of Homeland Security

- Recruited from the White House staff to be a member of the senior leadership team that built and launched the NCSD)/US-CERT.
- Named by Secretary Tom Ridge to be Acting Director of NCSD/US-CERT to lead the effort by the Department of Homeland Security to work collaboratively with government and private sector stakeholders to reduce risk in cyberspace and protect America's cyber assets (October 2004);
- Drafted a strategic plan to implement the cyber security mission pursuant to the authorities of the Homeland Security Act and Strategy, the National Cyber Strategy, and Homeland Security Presidential Directive-7.
- Managed the efforts of 30 government employees and over 125 contractors to address the overarching priorities of the strategic plan – to build a National Cyber Security Response System and a national cyber risk management program. Manage a FY 06 budget of over $100 million that grew from $79 million in FY05.
- Built a robust cyber security response system that entailed collaboration with the private sector and key government entities at the Federal, state, and local levels – and internationally – to build cyber situational awareness, attack attribution capabilities, coordinated response and mitigation capabilities, and the ability to reconstitute and recover after successful cyber attacks or the cyber consequences of cyber or physical attacks or natural disasters.
- Under the National Infrastructure Protection Plan, cyber risk management involved partnership with key government and private sector entities in the IT sector – and through lead agencies for other sectors – to identify assets and interdependencies, assess vulnerabilities and the consequences of their exploitation, and to assess cyber risk and the priority measures necessary to reduce that risk.
- Priority risk mitigation efforts included: Internet Disruption Working Group, Control Systems Security Program, and Software Assurance Security Program (including close partnership with the Office of Information Assurance of the U.S. Department of Defense).
- Co-Chair of the Committee on National Security Systems Working Group on Globalization of IT. Mission to address the security challenges to national security systems and critical infrastructure owners and operators posed by the increasing globalization of information technology.

[a] Deputy Director through September 2004.

Deputy to the Vice Chair (April 2002 to April 2003)
Senior Advisor for IT Security and Privacy[b]
Deputy to the Vice Chair
The President's Critical Infrastructure Protection Board (PCIPB)
The White House

- Advisor on privacy and cybercrime-related issues in formulation of the *National Strategy to Secure Cyberspace*.
- Leadership role in the following strategic and implementation issues:
  - enhancing the cybersecurity of the financial services sector;
  - government procurement of secure IT;
  - creation of a government cyber incident sharing and analysis consortium;
  - Education committee's priorities involving creation of a national cybersecurity academy and the initiative to facilitate the formation of a private, independent body for the certification of IT professionals; and
  - development and improvement of cybersecurity awareness and education efforts.

Frequent speaker on behalf of the White House to further stakeholder engagement in the development of the Strategy and to raise cybersecurity awareness.

Chief Deputy General Counsel (1987 to April 2002)[c]
(Acting General Counsel, Nov. 1999 to Jan. 2001)
United States Sentencing Commission

- As a member of the senior management team, provided legal, strategic, administrative, and ethical advice to chair and commissioners, staff director and unit chiefs.
- As Acting General Counsel led the Commission through the historic 2000 and 2001 amendment cycles highlighted by promulgation of the economic crime amendments that dramatically restructured penalties for economic and new technology offenses across the nation.
- Developed expertise on the compliance plans incentivized by the Corporate Guidelines.
- As chief counsel for new technology issues, organized the National Symposium on Sentencing Policy for Economic Crimes and New Technology Offenses (10-01)
- Vice Chair/contract manger for the acclaimed 1995 national conference "Corporate Crime in America: Strengthening the 'Good Citizen' Corporation."
- Frequent speaker and trainer for federal judges, attorneys, and probation office.

[b] On detail from the Sentencing Commission.
[c] On detail to the White House.

Counsel (July 1989 to October 1989)[d]
U. S. Senate Impeachment Trial Committee
(Articles Against Judge Walter Nixon)

- Developed committee strategy and procedure.
- Explored the factual and legal issues raised by pre-trial motions and hearings.
- Briefed the full committee in closed meetings and by written memoranda.
- Advised committee members and staff during the trial, and during the Senate Executive Session.
- Co-drafted the committee's report to the full Senate.

Producer for News and Politics (1984-1987)
CBS News nightly broadcast NIGHTWATCH

- Covered national news stories for the Washington Bureau of CBS News (August 1986 on).
- As Producer for News and Politics for the CBS News broadcast NIGHTWATCH, with Charlie Rose,
  - managed news and political coverage and supervised fifteen professional staff members;
  - produced three two-hour specials on law-related issues: police corruption in Philadelphia, organized crime (hosted by Fred Graham), and the Chicago police.

Investigative Producer (1982-1984)
NBC News Magazines

- Managed breaking news coverage and produced news stories for the NBC News Washington Bureau (April to October, 1984).
- Covered national news events, conducted interviews, and produced and packaged news stories for NIGHTLY NEWS, THE TODAY SHOW, NBC NEWS AT SUNRISE, MONITOR and FIRST CAMERA (Consultant/Associate Producer to news magazines from November '82 to April 84).

Special Counsel (July 1982 to November 1982)
Committee on Standards of Official Conduct
U.S. House of Representatives

- Led congressional investigation of then-Rep. Fred Richmond (D-NY) into allegations of securities, tax, and other violations.
- Led investigative stage of allegations of drug and sexual abuse of Capitol Hill Pages.

[d] On detail from the Sentencing Commission.

Assistant United States Attorney (April 1979 to June 1982)
Eastern District of Pennsylvania (Philadelphia)
U.S. Department of Justice

- Prosecuted complex white collar crime cases, including: RICO, tax evasion and fraud, embezzlement, narcotics, complex financial fraud, and police corruption.
- Served as Special Assistant U.S. Attorney in Miami (1980) and Atlanta (1981).
- Instructor at the Attorney General's Trial Advocacy Institute.
- Received Outstanding Achievement Award from the U.S. Department of Justice for successful nine-week trial in Atlanta of a $20 million RICO fraud case.

Senior Staff Counsel (December 1976 through December 1978)
Select Committee on Assassinations
U.S. House of Representatives

- Led the investigation into the possibility that Jack Ruby conspired with Lee Harvey Oswald, or others, to kill President John F. Kennedy.
- Led inquiry into the medical/autopsy evidence to determine if there was only one gunman.

EDUCATION

University of Virginia School of Law
Juris Doctor

College of William and Mary
B.A. High Honors (Govt.-Economics)

BAR MEMBERSHIP (INACTIVE)
Washington, D.C., Maryland, Missouri, Pennsylvania

HOBBIES: GOLF, SURFING, AND WORKING OUT.

PUBLICATIONS AND REFERENCES AVAILABLE UPON REQUEST

EXHIBIT B

April 4, 2013

The Honorable John Boehner
Speaker of the House
U.S. House of Representatives
Washington, DC 20515

The Honorable Nancy Pelosi
Democratic Leader
U.S. House of Representatives
Washington, DC 20515

The Honorable Harry Reid
Majority Leader
U.S. Senate
Washington, DC 20510

The Honorable Mitch McConnell
Republican Leader
U.S. Senate
Washington, DC 20510

Dear Speaker Boehner, Democratic Leader Pelosi, Majority Leader Reid, and Republican Leader McConnell:

The undersigned associations are writing to express our concern with language included in Section 516 of P.L. 113-6, the Consolidated and Further Continuing Appropriations Act for Fiscal Year 2013, which was signed into law by President Obama on March 26, 2013. This provision will bar the Departments of Commerce and Justice, the National Aeronautics and Space Administration, and the National Science Foundation from acquiring information technology (IT) systems unless "the head of the entity, in consultation with the Federal Bureau of Investigation or other appropriate Federal entity" has made a risk assessment of potential "cyber-espionage or sabotage...associated with such system being produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China." Given the expedited manner in which this provision was enacted, we ask the Congress to review the security implications and competitive impact of this requirement, and consider a more constructive approach to this issue. We also seek your support to ensure similar language is not included in other legislative vehicles.

Our associations represent thousands of U.S. technology companies. As designers, producers and consumers of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy and are aligned with the U.S. and other governments' goals to enhance cybersecurity. We understand and share Congress' concern about the security of the U.S. government's IT infrastructure.

The IT assessment requirements in Section 516, however, set a troubling and counterproductive precedent that could have significant international repercussions and put U.S.-based global IT companies at a competitive disadvantage in global markets. Fundamentally, product security is a function of how a product is made, used, and maintained, not by whom or where it is made. Geographic-based restrictions run the risk of creating a false sense of security when it comes to advancing our national cybersecurity interests. At a time when greater global cooperation and collaboration is essential to improve cybersecurity, geographic-based restrictions in any form risk undermining the advancement of global best practices and standards on cybersecurity.

We are concerned Section 516 could result in the following:

- Impede the U.S. government's ability to protect itself through use of the latest cutting-edge IT products. The requirement to assess every IT product purchase, absent any triggering threshold, will likely slow the federal acquisition process and put impacted federal agencies behind the security innovation curve because they would not be acquiring and using the latest security innovations.

- Put federal civilian agencies in conflict with the Department of Defense's (DoD) cybersecurity procurement reforms. The recent *Department of Defense Strategy for Operating in Cyberspace* recommended reforming the acquisition process, stating "DoD's acquisition processes and regulations must match the technology development life cycle. With information technology, this means cycles of 12 to 36 months, not seven or eight years."
- Fuel potential retaliation. The Chinese government may choose to retaliate against U.S.-based IT vendors by enacting a similar policy for screening IT system purchases in China.
- Encourage copycat legislation. Governments in other countries may seek to emulate this policy, harming U.S. IT vendors who wish to sell in those markets. Similar policies are already being pursued by some foreign governments. We are concerned this provision would severely undermine the U.S. government's efforts to contain these policies.

U.S. IT companies' significant global sales contribute substantially to the revenue we invest in domestic R&D, and new products and services. All of our members have a shared commitment to ensure their IT products and services reflect the latest and greatest in cybersecurity protection, and that cybersecurity policies advance this goal while maintaining our companies' innovative and competitive potential in global markets. Section 516 creates challenges that could undermine U.S.-based companies' global competitiveness.

Section 516 was not subject to committee hearings or markup, and was included in must-pass funding legislation that went through an expedited legislative process with limited opportunities for amendment. The global IT sector is committed to working with Congress and the Administration to consider constructive approaches that avoid geographic-based restrictions and focus instead on the appropriate and effective methods to meet our cybersecurity challenges. In the near term, we strongly encourage a meaningful bilateral dialogue between the United States and China to address cybersecurity concerns in a manner consistent with best security and trade practices.

Sincerely,

BSA | The Software Alliance
Emergency Committee for American Trade (ECAT)
Information Technology Industry Council (ITI)
Semiconductor Industry Association (SIA)
Software & Information Industry Association (SIIA)
TechAmerica
Technology CEO Council
Telecommunications Industry Association (TIA)
U.S. Chamber of Commerce
U.S. Council for International Business (USCIB)
U.S. Information Technology Office (USITO)

CC: J. Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, Executive Office of the President

EXHIBIT C

REPLY DECLARATION OF THOMAS DOWDING

I, Thomas Dowding, hereby declare, affirm, and state the following:

I. Introduction

1. I am over the age of eighteen and I am a citizen of the United States.

2. The facts set forth below are known to me personally, and I have firsthand knowledge of them.

3. I am Senior Vice President of Sales, Wireless Business and the Smart PV Plant Solution Division of Huawei Technologies USA, Inc. ("Huawei Technologies USA"), which is a subsidiary of Huawei Technologies, Co., Ltd ("Huawei").

4. I make this declaration in support of reply comments submitted by Huawei Technologies USA in response to a Notice of Proposed Rulemaking ("NPRM") issued by the Federal Communications Commission ("FCC") in WC Docket No. 18-89 on April 18, 2018, and comments filed in the record by various parties as of June 1, 2018.

5. I hereby incorporate by reference my prior Declaration, submitted as Exhibit C to the Comments of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., filed on June 1, 2018 in Docket No. 18-89.

II. Huawei Product Security

6. Huawei offers a diverse variety of telecommunications equipment, all of which is designed and developed with cybersecurity protections.

7. In the United States, Huawei Technologies USA offers telecommunications equipment to its carrier and enterprise customers, including radio access network products, broadband access network services, core network products, Internet Protocol ("IP") routers and

gateways, WLAN solutions, Ethernet switches, high-performance servers, carrier-grade transport products, storage, Software Defined Network ("SDN"), management systems and software, and technical service solutions for customer services.

8. Huawei Technologies USA does not manage networks or provide services that involve storing the end user data of its carrier and enterprise customers in a manner that would give Huawei Technologies USA access to its customers' network information. All network and user data is entirely controlled by the customers and cannot be accessed by Huawei Technologies USA without prior written customer consent.

9. Huawei takes seriously its responsibility to design secure products and services and embraces the concept of "security-by-design." Huawei remains focused on security from the beginning of the design phase throughout the product and/or service lifecycle. Huawei includes a product's baseline security requirements in the initial list of requirements for a new product under development. In addition, Huawei works with capable customers to include a threat analysis of scenarios based on the particular customer's site or customer-specific security requirements. Security threats identified in the concept phase are then further specified in the planning phase as the product design becomes more detailed and product security architecture and security design features are designed. During the development phase, product developers follow secure coding specifications when writing and reviewing software, and automatic scanning tools are used to reduce security defects and identify areas for further investigation. Finally, most products are tested based on the security baseline and threat models by Huawei's internal Cyber Security Lab, which is independent from the Research & Development team.

10. If the internal Cyber Security Lab evaluates any product as "high risk," Huawei Global Cyber Security Officer has the right to veto the release of this product. Moreover, Huawei traces security requirements forward from the original requirements through to the final product, and back again in reverse, to cover all steps, processes, individuals, components, vendors and versions involved in development.

11. In addition, many Huawei products are intrinsically secure because they are incapable of routing or redirecting user data traffic or because they do not permit visibility into data or packets transmitted or handled by such equipment. These products include antennas, inverters, power supplies, cabinets and storage disk arrays, etc.

12. Huawei products are utilized by multiple U.S. wireline and wireless carriers, many of whom rely on Huawei's affordable, reliable equipment in order to provide telecommunications services to remote or rural areas.

13. In my 15-year tenure of executive positions at Huawei Technologies USA, the U.S. Government has never identified any particular deliberately compromised Huawei product. Likewise, I am not aware of any product backdoor identified by the U.S. Government to our customers. Also, the U.S. government has never requested a forensic examination of any Huawei product for security vulnerabilities. But the U.S. government is not alone. In fact, I'm not aware of any government in any country that has ever found an implanted backdoor in any of our products.

VII. Conclusion

14. A blanket ban of all Huawei products would deprive the U.S. market of cost-effective telecommunications equipment which pose no threat to national security, including

inherently secure products that cannot route or redirect user data traffic or permit visibility into any user data or packets transmitted or otherwise handled by the product.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on July 2, 2018.

Thomas Dowding

EXHIBIT D

Before the
Federal Communications Commission
Washington, D.C. 20554

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

Reply Declaration of Allan L. Shampine

June 29, 2018

I. INTRODUCTION

1. My name is Allan L. Shampine. I have previously submitted a declaration in this proceeding dated May 30, 2018.[1] My qualifications are provided in that declaration, which I incorporate here by reference.

2. I have been asked by counsel for Huawei to review the economic analysis concerning competition for telecommunications equipment in the Comments of the Telecommunications Industry Association ("TIA").[2] I make three points about their comments:

- TIA sets up a strawman in its discussion of competitive conditions. The relevant question is not whether there would be at least one seller of equipment left in the event of regulatory intervention, but whether allowing Huawei to compete freely in the marketplace would benefit consumers.

- TIA is advocating to exclude by regulatory *fiat* a firm that competes with its members.

- TIA does not address the fact that existing Huawei customers, and those that have benefited from Huawei bidding for their business, are disproportionately concentrated in rural areas, including ones with relatively poor wireless and Internet access. Those consumers would be directly disadvantaged if they were prevented from working with Huawei.

---

1. Declaration of Allan L. Shampine, WC Docket No. 18-89, May 30, 2018 ("Shampine Declaration"), in relation to Federal Communications Commission, In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, FCC 18-42, WC Docket No. 18-89 (released April 18, 2018) ("NPRM").

2. Cinnamon Rogers, Dileep Srihari, K.C. Swanson and Savannah Schaefer, Comments of the Telecommunications Industry Association, WC Docket No. 18-89, June 1, 2018, https://ecfsapi.fcc.gov/file/1060164707659/TIA%20USF%20Security%20Comments%206-1-18.pdf, ("TIA Comments"), pp. 71-77.

3. After reviewing the TIA Comments, I reach the same conclusion that I articulated in my prior declaration. Allowing Huawei to compete more freely in the United States could create significant consumer benefits. I explain in more detail below.

II. ALLOWING HUAWEI TO COMPETE MORE FREELY IN THE UNITED STATES COULD CREATE SIGNIFICANT CONSUMER BENEFITS

4. In addressing competitive conditions, TIA essentially sets up a strawman in its Comments, answering an irrelevant question. The TIA Comments claim that "there are sufficient options available to fixed and mobile broadband providers in order for such companies to meet their universal service obligations" through purchases from TIA's membership.[3] Even if true, this claim by itself is insufficient to address the Commission's questions about the costs of its proposed policy. The relevant question is on what terms those purchases will be made – what impact can be expected from excluding significant competitors from the industry? Claims that there are multiple firms that sell certain pieces of equipment do not by themselves address that question. Indeed, the same claim that TIA advances could be made if regulators were contemplating barring all but one firm from the industry, leaving a monopoly supplier. That is, so long as there is at least one supplier, carriers will be able to purchase equipment and "meet their universal service obligations." Excluding a significant competitor, however, can still harm consumers by denying the benefits of that firm competing for their business.

5. To see why, consider the Federal Trade Commission's ("FTC") challenge of the US Foods and Sysco merger. This was a merger of two foodservice distribution companies. As the two companies pointed out, there are a huge number of companies distributing food, and those companies collectively have sales much larger than the two parties attempting to merge.[4] However, the FTC responded, and the District Court agreed, that suppliers can differ in important ways beyond just their product offerings. Specifically, the District Court had to define

3. TIA Comments, p. 77.

4. United States District Court for the District of Columbia, Memorandum Opinion, Federal Trade Commission, *et al.*, v. Sysco Corporation, *et al.*, Civil No. 1:15-cv000256 (APM), June 29, 2015 ("FTC Sysco Opinion"), p. 19.

a "product market," which in economic terms means defining the products and firms that are sufficiently close competitors that they constrain one another's pricing. The "product" need not be a discrete good for sale.[5] The FTC claimed, and the District Court agreed, that the relevant product market was "broadline" food distribution – characterized by "a vast array of product offerings, private label offerings, next-day delivery, and value-added services" with "geographically dispersed distribution centers" where customers can "make purchases under a single contract that offers price, product, and service consistency across all facilities," with contracts awarded "through a request for proposal or bilateral negotiations."[6] The District Court found that although there was no question that smaller firms, niche firms, regional firms, and other types of firms also provided food distribution services, those other firms nonetheless did not constrain the prices of the "broadline" food distributors – that is, they were not in the same relevant economic market.[7]

6. Similarly, in this proceeding the TIA Comments list a variety of firms that they claim sell telecommunications infrastructure (discrete products), but that does not mean that they are all in the same relevant market. Indeed, the TIA Comments list several discrete types of infrastructure, then follow that list with a separate list of firms that it claims offer such services, but it is not the case that each firm listed offers each of the types of infrastructure listed. For example, the TIA Comments list Dell.[8] Dell sells computer equipment. It does not sell wireless infrastructure, nor many other kinds of telecommunications infrastructure. Indeed, Dell's 2017 10-K does not even contain the word "wireless."[9] Similarly, the TIA Comments list Juniper and Cisco,[10] but the European Commission has noted that Juniper and Cisco participated in "the markets for routing

5. FTC Sysco Opinion, p. 21.

6. FTC Sysco Opinion, pp. 18-19, 41.

7. FTC Sysco Opinion, pp. 18-41.

8. TIA Comments, p. 76.

9. Dell 10-K for the Fiscal Year ended February 3, 2017, https://www.sec.gov/Archives/edgar/data/1571996/000157199617000004/delltechnologiesfy1710k.htm.

10. TIA Comments, p. 73.

and switching solutions" but were not "integrated in RAN [Radio Access Network] and CNS [Core Network Systems]."[11]

7. The European Commission examined separate economic markets for wireless RAN equipment; CNS equipment; Deployment, Delivery and Installation services; and Network Infrastructure Services; along with segments of each of those categories.[12] As I described in my prior declaration, the European Commission listed a small number of firms as providing credible alternatives for customers in each market after the proposed Nokia/Alcatel merger.[13] That list for RAN equipment, for example, was comprised of Ericsson, Huawei, ZTE and Samsung.[14]

8. Similarly, most of the firms listed in the TIA Comments do not appear in market research reports for the relevant market segments. For example, the Gartner Group's analysis of LTE network infrastructure lists four firms as having a combination of ability to execute and completeness of vision – Ericsson, Nokia, Huawei and ZTE. Gartner notes that while Cisco, a firm listed in the TIA Comments, provides some RAN equipment, its portfolio does not include macrocell/microcell base stations, and it cannot fulfill carriers' requirements there.[15]

9. Thus, the fact that a firm sells some pieces of infrastructure equipment does not mean that it is a significant competitive constraint on "full line" firms like Huawei that can, and do, bid for complete network upgrades and construction of entirely new networks. As the European Commission noted when evaluating the Nokia/Alcatel merger, contracts for network upgrades

---

11. European Commission, Case No COMP/M.7632 – Nokia / Alcatel-Lucent, Regulation (EC) No 139/2004 Merger Procedure, Article 6(1)(b) Non-Opposition, July 24, 2015, document number 32015M7632, http://ec.europa.eu/competition/mergers/cases/decisions/m7632_788_2.pdf, ("EC Nokia/Alcatel Decision"), ¶ 210.

12. EC Nokia/Alcatel Decision, § 4 – Relevant Markets.

13. Shampine Declaration, § IV.

14. See, for example, EC Nokia/Alcatel Decision, ¶¶ 96-98.

15. Kosei Takiishi, Sylvain Fabre, Peter Liu, Frank Marsala & Jessica Ekholm, "Magic Quadrant for LTE Network Infrastructure," Gartner, July 31, 2017, pp. 2-3.

tend to be large, infrequent, and often awarded to a single bidder.[16] I also noted in my prior declaration that combining equipment from multiple manufacturers can be difficult and costly,[17] but that firms were seeking to do so regardless specifically because of concerns about "a consolidated RAN vendor landscape." Industry consulting firm GlobalData noted specifically that, "It's also not surprising to see U.S. operators as key instigators in this movement, given that – with meaningful access to Huawei and ZTE blocked for political reasons – they face the fewest options for RAN gear."[18]

10. Further evidence is provided in declarations submitted by rural carriers noting that their networks are comprised largely or entirely of equipment purchased from Huawei, and that if they lost access to that vendor they would have to "rip and replace" the network. The statements of these carriers contradict the claim in the TIA Comments that Huawei and ZTE's competition is irrelevant and that many firms stand ready to serve all carriers. For example, one of the commenting rural carriers notes that the only response it received to its request for proposal for its network was from Huawei.[19] And they all note that they received better terms and service as a result of Huawei's bidding for their business.[20]

16. EC Nokia/Alcatel Decision, ¶¶ 18, 87, 96.

17. See also Steven Berry, Rebecca Thompson, Courtney Neville, Theodore Olson, Thomas Dupree, Jr., and Andrew Kilberg, Comments of Competitive Carriers Association, June 1, 2018 ("CCA Comments"), pp. 9-10 (stating that the only practicable solution for most carriers will be to "rip-and-replace" existing equipment with new equipment due to the uncertainty regarding interoperability); Comments of Mark Twain Communications Company, June 1, 2018, p. 5 (expressing concern that some rural carriers' equipment may not be able to interoperate with new equipment from another supplier); and Comments of Pine Belt Cellular, Inc., June 1, 2018, p. 6 (expressing concern about long-term interoperability if Pine Belt were to continuing using existing equipment from the targeted companies with equipment from different manufacturers).

18. Ed Gubbins, "MWC18: The Radio Access Network Roundup – As 5G Dawns, Integrating Massive MIMO & Breaking Up the RAN," GlobalData, March 7, 2018.

19. Declaration of Eric J. Woody, Union Telephone Company, attached to Comments of Competitive Carriers Association, June 1, 2018, ¶ 3.

20. CCA Comments, June 1, 2018, attached declarations.

- SI Wireless states that the majority of its network has been constructed with Huawei equipment, chosen because of its cost-effectiveness, excellent quality, and excellent customer service, and that prohibiting Huawei equipment and services would require SI Wireless to replace that network at a cost of $40 to $60 million.[21]

- NE Colorado Cellular states that roughly 80 percent of equipment in its network comes from Huawei, chosen because it was the most cost-effective option and because of Huawei's customer service, and that prohibiting Huawei equipment and services would require NE Colorado Cellular to "rip and replace" much of its network at a cost of more than $400 million. NE Colorado Cellular also noted that it would expect additional and ongoing costs from higher servicing costs, and having to use inferior equipment with less responsive customer service from other equipment manufacturers.[22]

- James Valley Telecommunications states that 100 percent of its wireless core network and wireless radios are from Huawei, that it obtained 40 percent savings relative to the next most cost-effective option, and that prohibiting Huawei equipment and services would require it to undertake network replacement costs of roughly $5,000 per customer. Given roughly 10,000 predominantly rural customers, all of whom James Valley Telecommunications provides LTE service to using Huawei equipment, that yields $50 million.[23]

21. Declaration of Michael Beehn, SI Wireless LLC, attached to CCA Comments, June 1, 2018, ¶¶ 4-5.

22. Declaration of Frank DiRico, NE Colorado Cellular, attached to CCA Comments, June 1, 2018, ¶¶ 3-4.

23. Declaration of James Groft, James Valley Telecommunications, attached to CCA Comments, June 1, 2018, ¶¶ 2-4.

- United Telephone Association states that its wireless network consists primarily of Huawei equipment, which was technically superior to other options and was "by far" the most cost effective.[24]

- Nemont Telephone Cooperative states that over 70 percent of the wireless network of its subsidiary Sagebrush Cellular, Inc. comes from Huawei, and that it chose Huawei because of its technical capabilities, customer support, and cost effectiveness. Prohibiting Huawei equipment and services would require it to undertake network replacements costs of around $57 million, and there would likely be higher costs of materials, support and upgrades going forward.[25]

- Union Telephone Company states that roughly 75 percent of its network equipment comes from Huawei. It also states that Huawei was the only vendor to respond to its request for proposal after the previous vendor was found to be unsatisfactory, and that Huawei is highly cost-effective and provides excellent customer service. Union Telephone Company estimates the costs of the Commission's proposed rule to be around $340 million in direct, "start-up" costs, with ongoing higher service costs and decreased quality.[26]

11. As I discussed in my prior declaration, the Chief Technical Officer of Telus has estimated that Huawei's presence in the market "dropped prices by 15% at least" as Ericsson and Nokia were forced to respond.[27] James Valley Telecommunications' declaration, discussed above, indicated that Huawei's bid was 40 percent below competing offers.[28] My own analysis of

---

24. Declaration of Todd Houseman, United Telephone Association, Inc., attached to CCA Comments, June 1, 2018, ¶ 3.

25. Declaration of Michael Kilgore, Nemont Telephone Cooperative, Inc., attached to CCA Comments, June 1, 2018, ¶¶ 2-3.

26. Declaration of Eric Woody, Union Telephone Company, attached to CCA Comments, June 1, 2018, ¶¶ 3-5.

27. Shampine Declaration, ¶ 21.

28. Declaration of James Groft, James Valley Telecommunications, attached to CCA Comments, June 1, 2018, ¶ 3.

concentration and prices for RAN equipment generally and for LTE base stations specifically (evolved NodeBs, or eNodeBs) is consistent with these conclusions. For example, industry concentration is higher in North America than elsewhere in the world (e.g., Europe), and average selling prices per LTE base station (whether overall, or by pico, micro and macro individually) are higher in North America than in any other region of the world. I calculate that the differences are all at least as large as those described by Telus, and many are as large or larger than those described by James Valley Telecommunications.[29]

12. The TIA Comments also claim that "Huawei products reportedly make up *less than one percent* of the equipment in American cellular and landline networks today."[30] However, this claim does not address the question of the competitive significance of Huawei either currently or in the future. As I explained in my prior declaration and above, in situations where there are large, infrequent contracts put out to bid, a low share may understate a firm's competitive significance. That is, there may be few firms that can bid on such large contracts, and the loss of one or more firms because of regulatory *fiat* can have a significant impact on the resulting prices and terms. This is true even if the firm(s) in question had a very small market share before the regulatory decision to exclude them. Furthermore, as discussed above and further below, Huawei has a disproportionate presence in rural areas with relatively poor wireless and Internet access. Exclusion of Huawei entirely from the United States would thus have a disproportionate impact on those areas. Furthermore, bidding competition from Huawei can force other firms to lower prices and provide better terms to carriers, even if the business does not ultimately go to Huawei, and such price concessions can result in benefits to other carriers because of, for example, "most favored nation" clauses in their own contracts. That is, if a firm like Ericsson competes with Huawei for a contract with a rural carrier, and makes price and term concessions

29. Based on analysis of data from market research firms Infonetics, IHS, and Dell'Oro, news reports, and the European Commission and MOFCOM. See Shampine Declaration § IV.

30. TIA Comments, p. 71. Emphasis in original.

to win the contract, other carriers may in turn benefit from those concessions if they have most favored nations clauses in their own contracts.[31]

13. Thus, when Huawei bids for the business of firms, those firms benefit even when they do not finally make the purchase from Huawei. To be clear, they benefit because competitors like Nokia and Ericsson have to take Huawei's presence into account when developing their own bids. Furthermore, those firms that do actually make their final purchases from Huawei are clearly harmed if they suddenly become barred from doing further business with Huawei. Indeed, the source that the TIA Comments cites for the 1 percent share was specifically making the point that Huawei "has been actively courting small-town internet companies that wanted to replace old-fashioned landlines with high-speed internet connections—no small feat in a country where most rural residents are stuck with dial-up speeds. … Many of these customers now worry the new heat over Huawei in Washington may rob them of what has so far been an important alternative to Western suppliers. Others worry that if Huawei exits the U.S. completely, it will leave them without the customer and technical support they need to maintain the Huawei hardware they already own."[32] That is, the Wall Street Journal article cited by the TIA Comments to support the claim that Huawei's presence in the U.S. is insignificant is actually making the opposite point – that Huawei has been providing assistance to communities that have historically been underserved with respect to landline and wireless broadband service, and that exclusion of Huawei from the U.S. will harm those communities.

14. Given the emphasis placed in the TIA Comments about how its members stand ready to serve consumers that would otherwise choose to purchase services from Huawei,[33] it is worth pointing out that while exclusion of a firm by regulatory *fiat* will benefit the competitors of that firm, the same cannot be said for consumers. For example, when evaluating a merger between

---

31. See, for example, Declaration of Steven Berry, attached to CCA Comments, June 1, 2018, ¶ 8, noting that some of the larger vendors include "most favored nation" clauses in their purchase contracts with certain carriers.

32. Drew Fitzgerald and Stu Woo, "In U.S. Brawl With Huawei, Rural Cable Firms Are an Unlikely Loser," The Wall Street Journal, March 27, 2018, https://www.wsj.com/articles/caught-between-two-superpowers-the-small-town-cableguy-1522152000.

33. TIA Comments, p. 77.

two firms, regulators recognize that complaints by competitors of those firms may actually indicate that the merger will benefit consumers by increasing competition. The declarations from Huawei customers provide further evidence of the competitive importance of Huawei when it is permitted to compete.

15. The benefits from increased competition can be substantial, particularly in concentrated markets. I discussed in my prior declaration that the DOJ and FTC Horizontal Merger Guidelines include a presumption of significant competitive effects from eliminating a competitor in a concentrated market.[34] How substantial might that effect be in this specific market? I noted in my prior declaration that in the United States, AT&T, Verizon, T-Mobile and Sprint have collectively reported 2018 capital spending of more than $50 billion.[35] With 5G deployments beginning, that figure may well increase in coming years. Taking the estimate of Telus' CTO that Huawei's participation in the infrastructure market can reduce prices by 15 percent, and applying it to an estimated 2018 capital spending level of $50 billion, that would be a benefit to customers of $7.5 billion in one year. Furthermore, five members of the Competitive Carriers Association discussed above estimated that those five alone would face costs around $900 million if Huawei were excluded entirely from competing in the United States.[36] They also all note that they received lower prices as a result of Huawei's competing for their business. One reported a 40 percent reduction in prices. I note that the costs for just those five carriers alone would total around twice the annual Mobility Fund Phase II budget of $450 million.[37] The GSM Association estimates carrier capital expenditures in North America for 2017 to 2020 to reach around $136 billion.[38] Even a 15 percent savings on that total from allowing Huawei to compete freely would amount to $20 billion. Note that this is just for wireless infrastructure. Huawei is

34. Shampine Declaration, ¶ 12.

35. Shampine Declaration, ¶ 24.

36. See ¶ 10, *supra*.

37. Federal Communications Commission, Connect America Fund; Universal Service Reform – Mobility Fund, Report and Order and Further Notice of Proposed Rulemaking, FCC 17-11, March 7, 2017, ¶ 23.

38. GSM Association, "The Mobile Economy North America 2017," https://www.gsmaintelligence.com/research/?file=b0cf4f71cb2d035f429d9de8ca4fc72e&download, p. 6.

also a significant provider worldwide in other areas, including smartphones, wireline infrastructure, and enterprise equipment and services, and increased competition in these other areas would create additional benefits.

16. Of course, the benefits of competition go beyond just price – firms also compete to offer better service, higher quality and more innovative products. For example, as discussed above, rural carriers seeking to upgrade networks in remote areas of the United States have been particularly pleased with not just the pricing, but also the quality and level of service provided to them by Huawei.

17. The TIA Comments' claim that exclusion of a significant competitor like Huawei from the U.S. market by regulatory *fiat* would be costless is without basis and inconsistent with the available evidence. To the contrary, the available evidence indicates that competition from Huawei benefits consumers in areas where it has been allowed to compete. Furthermore, as I discussed at some length in my prior declaration, increased prices and lower quality resulting from reduced competition can be expected to reduce investment in telecommunications infrastructure.[39] The declarations submitted by rural carriers make clear that this is not just a theoretical concern. The commenters state that not only does the proposal to remove Huawei entirely from competing in the United States raise concerns about their ability to maintain existing service coverage, expand their networks and upgrade to 5G, but that the uncertainty about Huawei's status is already deterring investment by these firms.[40] I discussed in my prior declaration the Commission's own concerns about underserved areas,[41] and the rural carriers' comments are consistent with those concerns.

39. Shampine Declaration, § V.

40. CCA Comments and attached declarations.

41. Shampine Declaration, ¶ 25.

I declare under penalty of perjury that the foregoing is true and correct. Executed on June 29, 2018.

_____

Allan Shampine