

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

**REPLY COMMENTS OF
THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

Cinnamon Rogers
Senior Vice President, Government Affairs

Dileep Srihari
Senior Policy Counsel and Director,
Government Affairs

K.C. Swanson
Director, Global Policy

Savannah Schaefer
Policy Counsel, Government Affairs

Colin Black Andrews
Policy Counsel, Government Affairs

TELECOMMUNICATIONS INDUSTRY
ASSOCIATION
1320 N. Courthouse Road
Suite 200
Arlington, VA 22201
(703) 907-7700

July 2, 2018

EXECUTIVE SUMMARY

The Telecommunications Industry Association (“TIA”) supports the Commission’s proposal to prevent the use of federal Universal Service Fund (“USF”) dollars to procure or obtain equipment or services produced or provided by certain suppliers deemed to pose a national security threat. The record of this proceeding shows that many commenters agree with TIA on several fundamental points:

- Protecting the security of communications networks is critical;
- Consumers, businesses, and community anchor institutions that rely on USF-supported networks and equipment will directly benefit from the assurance of secure communications;
- Consistent with its universal service statutory authority, the Commission should adopt a rule preventing USF support from being used to purchase equipment from companies that pose a national security risk;
- The Commission’s actions in this respect should be narrowly tailored and carefully targeted to that purpose; and
- Any Commission action should be taken in coordination with, and in reliance upon, determinations by other agencies within the federal government with national security expertise and access to pertinent classified information.

Contrary to claims made by some, the Commission is on the right path by focusing on specific suppliers of concern rather than cybersecurity supply chain risk management issues more generally. Importantly, a rule that relies on determinations made by national security agencies would complement, not undermine, a whole-of-government approach. Meanwhile, suggestions that industry standards or certifications can sufficiently address the threat posed by specific suppliers with strong ties to countries of concern miss the mark.

The record also shows that the benefits of a narrowly tailored rule would far outweigh the costs. Even a narrowly tailored rule would make a very meaningful contribution to national security. Although there could be some costs involved for a small number of companies that have already deployed problematic equipment in their networks, given the serious national security concerns at issue in this proceeding and given the highly competitive communications equipment marketplace, no cost assessment could ever validate endangering United States national security interests. The record – including additional information submitted by TIA with these reply comments – shows that adopting a narrowly tailored rule would only impact a small number of carriers. Moreover, USF recipients will continue to benefit from an equipment marketplace that remains robustly competitive across all market segments, including core equipment, wired and wireless access network infrastructure, end-to-end design and installation services, and support services. Nevertheless, TIA endorses consideration of targeted action by the Commission to provide some relief to USF recipients that may need to take steps to comply with the rule ultimately adopted by the Commission.

TIA urges the Commission to defer to expert judgments made by national security agencies regarding specific suppliers. That said, given the extensive submissions from one company that is a specific focus of concern, our comments provide additional information for the

record justifying the concerns raised about certain Chinese suppliers in the United States and elsewhere. Various strategic challenges regarding Chinese information and communications technology (“ICT”) companies, along with specific strong connections between Huawei, ZTE, and the Chinese state, provide legitimate grounds for the Commission to conclude – as have Congress and agencies of the Executive Branch – that a significant concern exists with regard to those companies. Simply put, the Commission has a valid basis for action, and nothing submitted undermines that basis.

Finally, by adopting a narrowly tailored rule as TIA has proposed, the various legal arguments raised against the Commission’s proposal would all be rendered moot. Contrary to claims by some commenters, the Commission has clear statutory authority under the Communications Act to adopt a targeted rule. Doing so would be in direct furtherance of established universal service principles and supported by clear precedent permitting the Commission to establish conditions on the receipt of USF support. The agency may also permissibly rely on determinations made by Congress or other agencies, and it may focus on the specific problem at hand (limited action concerning USF-supported equipment and services) without violating the Administrative Procedure Act. Finally, a narrowly tailored rule would be constitutional, as it would fully comport with the requirements of the Due Process Clause, the Takings Clause, and the Bill of Attainder Clause of the United States Constitution.

Since the opening comments were filed, TIA has continued to engage in active discussions with and among our member companies: the manufacturers and suppliers of the world’s ICT products. We have also continued to work with Congress and other stakeholders seeking to address these issues across the government. We look forward to working with the Commission as the agency considers its next steps on these very important issues in the months ahead.

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

TABLE OF CONTENTS..... iii

INTRODUCTION 1

DISCUSSION 3

I. COMMENTERS SUPPORT TARGETED ACTION BY THE COMMISSION THROUGH A NARROWLY TAILORED APPROACH PREMISED ON COORDINATION ACROSS THE FEDERAL GOVERNMENT. 3

 A. Commenters Agree That the Commission Should Draw From and Rely on the Expertise and Efforts of Other Government Actors Rather than Acting Unilaterally..... 4

 B. Commenters Also Widely Agree About the Importance of Protecting Communications Networks..... 7

II. A RULE FOCUSED ON SPECIFIC SUPPLIERS WOULD COMPLEMENT GENERAL SUPPLY CHAIN RISK MANAGEMENT EFFORTS..... 9

 A. Risks Posed by Specific Suppliers of Concern Are Distinct from Inherent Global Supply Chain Risks..... 9

 B. A Rule Focused on Specific Suppliers of Concern Would Not Interfere With General Supply Chain Risk Management Efforts By Government and Industry. 12

 C. A Rule Tied to Determinations Made by the Executive Branch or Congress Regarding Specific Suppliers Would Contribute to a Broader National Effort..... 14

 D. Supply Chain Standards and Certifications Are Not Designed to Address Risks Presented by Specific Suppliers Connected to Sophisticated State-Sponsored Actors. 17

III. THE BENEFITS OF A NARROWLY TAILORED USF RESTRICTION WOULD FAR OUTWEIGH ANY POTENTIAL COSTS..... 21

 A. A Narrowly Targeted Rule Would Provide Important Cybersecurity Benefits to USF Beneficiaries While Making a Meaningful Contribution to National Security... 23

 B. The Number of Affected Carriers Would Potentially Be Very Small and the Costs Would Be More Limited Than Certain Commenters Suggest. 28

 C. USF Recipients Will Continue to Benefit from a Competitive Vendor Market..... 31

1.	USF Recipients Have Many Options for Core Equipment, Wireless and Wireline Access Equipment, End-to-End Network Design and Installation Services, and Support Services.....	32
2.	Other Companies Provide Reasonably Comparable Alternatives for All Huawei Products Specifically Identified by Huawei.....	39
D.	The Commission Should Consider Remedial Steps for Affected USF Recipients While Taking Caution to Ensure Such Measures Do Not Undermine the Purpose of the Rule.....	41
IV.	COMPANIES SPECIFIED IN THE NOTICE MAY BE REASONABLY DISTINGUISHED FROM OTHERS DUE TO NATIONAL SECURITY CONCERNS. .	44
A.	The Record Regarding Specific Suppliers Named in the Notice Is Compelling.	46
B.	Significant Strategic Risks Have Been Identified Regarding the Chinese Government and Closely Connected ICT Companies.	49
C.	Huawei and ZTE Have Particularly Close Ties to the Chinese State.	57
D.	Huawei’s Statements Regarding Its Corporate Conduct Are Immaterial in the Proceeding at Hand.	69
V.	COMMENTERS THAT OPPOSE COMMISSION ACTION FAIL TO IDENTIFY CREDIBLE LEGAL BARRIERS TO THE ADOPTION OF A NARROWLY TAILORED RULE IN THIS CONTEXT.....	70
A.	The Communications Act Provides the Commission with Sufficient Statutory Authority to Adopt a Targeted USF Restriction.	71
1.	The Commission’s Adoption of a Targeted USF Restriction Is Rooted Squarely In Its Universal Service Authority.....	71
2.	Ensuring the Security of USF-Supported Networks is Consistent with the Universal Service Principles in Section 254(b) of the Act.....	75
B.	Adoption of a Narrowly Tailored Rule Would Not Be Arbitrary, Capricious, an Abuse of Discretion, or Otherwise Inconsistent with Law.	80
1.	The Commission May Permissibly Derive a List of Prohibited Suppliers from Determinations Made by Expert Agencies or by Congress.....	81
2.	The Commission Need Not Address All Supply Chain Security Issues at Once.....	86
3.	The Commission Has Provided Adequate Notice to Adopt Its Proposed Rule or Reasonable Variants Thereof.	88

C. A Narrowly Tailored Rule Would Be Constitutional.	91
1. To the Extent It Applies, the Due Process Clause Does Not Require an Individualized Hearing Before Adoption of a Rule of General Applicability Whose Implementation Is Guided By Determinations Made by Congress or by Other Agencies.	91
2. A Narrowly Tailored Rule Would Not Constitute a Regulatory Taking	96
3. The Rule Would Not Be a Bill of Attainder.	101
CONCLUSION.....	102
APPENDIX: Declaration of Cinnamon Rogers	

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

**REPLY COMMENTS OF
THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

The Telecommunications Industry Association (“TIA”)¹ respectfully submits these reply comments in the above-captioned proceeding.² As both an advocacy organization and a standards-setting body, TIA represents hundreds of global manufacturers and vendors of information and communications technology (“ICT”) equipment and services that are supplied to the owners and operators of communications networks, enabling operations across all segments of the economy.³

INTRODUCTION

The record in this proceeding shows that the majority of commenters agree with TIA that (i) protecting the security of communications networks is critical; (ii) consumers, businesses, and

¹ TIA is the leading trade association for the information and communications technology (“ICT”) industry, representing companies that manufacture or supply the products and services used in global communications across all technology platforms. TIA represents its members on the full range of policy issues affecting the ICT industry and forges consensus on voluntary, industry-based standards.

² *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC 18-42 (rel. Apr. 18, 2018), 83 Fed. Reg. 19,196 (May 2, 2018) (“Notice”).

³ As with TIA’s opening comments, these reply comments represent the views of the TIA Public Policy Committee. [Comments of the Telecommunications Industry Association](#), filed June 1, 2018 in WC Docket No. 18-89, at 1 n.3 (“TIA Comments”).

community anchor institutions that rely on USF-supported networks and equipment will directly benefit from the assurance of secure communications; (iii) consistent with its universal service statutory authority, the Commission should pursue its goals in this proceeding by adopting some form of rule preventing USF support from being used to purchase equipment from suppliers deemed to pose a national security risk; (iv) the Commission's actions in this respect should be narrowly tailored and carefully targeted to that purpose; and (v) any Commission action should be taken in coordination with, and in reliance upon, determinations by Congress or by other agencies within the federal government with national security expertise and access to pertinent classified information. Commenters also agree that the Commission should provide specificity and clarity in its final rule. TIA has offered rule text consistent with these widely shared views in its initial comments, which builds on the proposed rule in the Notice and provides the Commission with a concrete basis for further action.

Contrary to claims made by various commenters, the Commission is on the right path by focusing on specific suppliers of concern rather than cybersecurity supply chain risk management issues more generally. A rule that relies on determinations made by other agencies would complement, not undermine, a whole-of-government approach. Meanwhile, suggestions that industry standards or certifications can sufficiently address the threat posed by specific suppliers with strong ties to countries of concern miss the mark.

The record also shows that the benefits of a narrowly tailored rule would far outweigh the costs. Of course, given the serious national security concerns at issue in this proceeding, it is possible that no cost assessment could ever validate endangering United States national security interests. That said, the record – including additional information submitted by TIA with these reply comments – shows that adopting a narrowly tailored rule would impact a small segment of

the marketplace, and that impacted parties will benefit from an equipment marketplace that remains robustly competitive. However, TIA endorses consideration of targeted action by the Commission to provide some relief to USF recipients that may need to take steps to comply with the rule ultimately adopted by the Commission.

Although TIA has urged the Commission to defer to expert judgments made by national security agencies regarding specific suppliers, the extensive submissions from one company that has been a specific focus for concern – Huawei – merit a response. As shown below, the record justifying concerns regarding certain Chinese suppliers is significant, both in the United States and elsewhere. Various strategic challenges regarding Chinese companies, along with specific strong connections between Huawei, ZTE, and the Chinese state, provide legitimate grounds for the Commission to conclude that a significant issue exists.

Finally, the adoption of a narrowly tailored final rule as TIA has proposed renders moot all of the various legal arguments raised against the Commission’s proposal. The Commission’s proposed action is well within the statutory authority provided by the Communications Act and supported by the courts, would not violate the Administrative Procedure Act (“APA”), and presents no constitutional concerns.

DISCUSSION

I. COMMENTERS SUPPORT TARGETED ACTION BY THE COMMISSION THROUGH A NARROWLY TAILORED APPROACH PREMISED ON COORDINATION ACROSS THE FEDERAL GOVERNMENT.

The opening comments reveal some clear divisions regarding what specific action the Commission should take as a result of this proceeding. However, they also demonstrate broad agreement on certain principles that TIA identified in its opening comments as key guideposts as the Commission moves forward. As a result, the gap between those parties that support some

form of a USF restriction and those that do not is actually narrower than some commenters would suggest. This common ground offers a foundation on which the Commission can seek to develop a solution that accounts for the concerns of all stakeholders.

A. Commenters Agree That the Commission Should Draw From and Rely on the Expertise and Efforts of Other Government Actors Rather than Acting Unilaterally.

Fundamentally, no commenter suggests that the Commission can or should go it alone in seeking to defend communications networks from national security threats. On the contrary, *all* parties agree with TIA that the Commission should proceed only in close coordination with the various other governmental entities that are undertaking related initiatives, in order to preserve a whole-of-government approach. Notably, that consensus includes the Commission itself, as both the Notice and the Chairman’s separate statement disclaim any prospect of the Commission venturing out on its own to advance an independent security agenda.⁴

As TIA has explained, the Commission is not well positioned to perform national security evaluations of particular suppliers.⁵ TIA further observed that even if the Commission possessed the expertise and access to classified information required to make such determinations, it should not proceed independently, as doing so would result in a patchwork of different restrictions imposed by various corners of the government.⁶ Thus, TIA urged the Commission to rely on determinations made by expert security agencies or statutory requirements from Congress.⁷ In

⁴ Notice ¶ 2 (stating that the Commission has a “supporting” role to play); *id.*, Statement of Chairman Ajit Pai at 41 (“[T]he FCC doesn’t have the authority or capacity to solve this problem alone.”).

⁵ TIA Comments at 59-60.

⁶ *Id.* at 60.

⁷ *Id.* at 55-58.

fact, TIA outlined an interagency process that would protect the integrity of U.S. networks through a “whole of government” approach in which agencies would leverage their respective areas of expertise in a complementary manner.⁸

These same themes are echoed in comments from both sides of the debate in this proceeding. Commenters that endorse a USF restriction make clear that their support is contingent on any such action being a targeted part of a broader, coordinated effort that acknowledges and draws from other activities across the government.⁹ In fact, many of these parties advise the Commission to relinquish any presumption of primacy in connection with efforts to secure the communications supply chain to the Department of Homeland Security (“DHS”), as the Sector Specific Agency for both the communications and information technology (“IT”) sectors. As CTIA explains, DHS is well positioned to lead further efforts in this space because of its expertise, access to classified intelligence information, and ability to

⁸ See generally *id.* at 77-84.

⁹ See, e.g., [Comments of the Computer & Communications Industry Association](#), filed June 1, 2018 in WC Docket No. 18-89, at 6 (the Commission should proceed “carefully and in coordination with other government and industry partners,” to create a more comprehensive policy) (“CCIA Comments”); [Comments of EchoStar Satellite Operating Corporation and Hughes Network Systems, LLC](#), filed June 1, 2018 in WC Docket No. 18-89, at 7-8 (the Commission “should draw on coordinated efforts throughout the government so supply chain security requirements for USF recipients are aligned with and derive from broader interagency processes, national security decisions, or statutory requirements”) (“EchoStar/Hughes Comments”); [Comments of NTCA–The Rural Broadband Association](#), filed June 1, 2018 in WC Docket No. 18-89, at 9 (the Commission should coordinate action with various agencies, the intelligence community, and other sectoral regulators in order to avoid “[p]iecemeal approaches” that create “inconsistent policy implementation and overlapping regulatory burdens”) (“NTCA Comments”); see also [Comments of Motorola Solutions, Inc.](#), filed June 1, 2018 in WC Docket No. 18-189, at 4 (“Motorola Comments”); [Comments of NCTA – The Internet & Television Association](#), filed June 1, 2018 in WC Docket No. 18-89, at 6-7 (“NCTA Comments”); [Comments of USTelecom – The Broadband Association](#), filed June 1, 2018 in WC Docket No. 18-89, at 3-5 (“USTelecom Comments”).

protect confidential information shared by the private sector.¹⁰ Others agree.¹¹ Numerous comments also note the need to ensure consistency with the ongoing activities of other agencies including the Department of Commerce (“DOC”) (specifically including the National Telecommunications and Information Administration (“NTIA”) and the National Institute of Standards and Technology (“NIST”)), the Department of Justice (“DOJ”), and the Department of Defense (“DOD”).¹²

Notably, opponents of Commission action make this same case for Commission restraint. The Competitive Carriers Association (“CCA”), for example, says it is “ill-advised” for the Commission to attempt to make complex national security determinations on its own, and that it should allow DHS to take the lead on issues pertaining to supply chain security.¹³ As demonstrated above, CCA’s perceived adversaries in this proceeding concur with that assessment. And NTCA states that DHS, in collaboration with the intelligence agencies, is well positioned to lead this activity.¹⁴ That view is a common theme among all commenters.

This broad agreement on the scope of the Commission’s role is a rare luxury in a contemporary rulemaking. Rather than facing a choice between two starkly different regulatory visions, the Commission here is presented with a unanimous view that it should occupy, at most,

¹⁰ [Comments of CTIA](#), filed June 1, 2018 in WC Docket No. 18-89, at 2, 8 (“CTIA Comments”).

¹¹ *See, e.g.*, USTelecom Comments at 3 (the Commission should rely heavily on other federal agencies, particularly DHS, to make determinations about appropriate prospective restrictions and remedial measures); NCTA Comments at 9-10 (urging the Commission to proceed only pursuant to statutory guidance from Congress or formal guidance “deriving from a DHS-led interagency process”).

¹² CTIA Comments at 10-12; Motorola Comments at 3; NCTA Comments at 6-7.

¹³ [Comments of Competitive Carriers Association](#), filed June 1, 2018 in WC Docket No. 18-89, at 5, 22 (“CCA Comments”).

¹⁴ NTCA Comments at 22.

narrow ground in a crowded agency landscape – which is precisely what the Commission proposed. The divergence among commenters here concerns only the extent to which the Commission should defer to those other governmental efforts – that is, whether it should rely on expert security agencies to assist it in executing a narrowly defined task that falls uniquely within its jurisdiction, or whether it should, in the words of one commenter, simply “step back” and abdicate its responsibilities entirely.¹⁵ The record here clearly supports the former option.

B. Commenters Also Widely Agree About the Importance of Protecting Communications Networks.

Likewise, commenters broadly share the Commission’s interest in protecting the nation’s communications networks against security threats – particularly those networks that are supported by universal service funding.¹⁶ As TIA has explained, USF-funded networks are pervasive, and they interconnect indiscriminately with the rest of the vast communications infrastructure that supports connectivity for all Americans and with global commercial networks as well.¹⁷ Accordingly, promoting the security of these networks is critical for national security in general.¹⁸

¹⁵ *Id.* at 22.

¹⁶ Notice ¶ 34 (referencing “our goal of addressing national security threats to communications networks and the communications supply chain”).

¹⁷ TIA Comments at 6-8.

¹⁸ *Id.* at 6.

The other opening comments demonstrate a common appreciation for this goal¹⁹ – including among opponents of Commission action. For instance, PRTC “supports efforts to ensure that USF funds are not used in a manner inconsistent with national security.”²⁰ RBA “fully supports efforts to improve national security.”²¹ TracFone observes that “[o]ur communications networks play a critical role in protecting public safety and national security.”²² Even CCA, one of the most fervent detractors of the Commission’s proposed actions, deems the agency’s intentions in this proceeding to be “laudable.”²³

The proposition that it is critical to protect the nation’s communications networks should, of course, be noncontroversial. But the fact that it is recognized explicitly on both sides of this debate stands as an endorsement of the Commission’s intentions in this proceeding, even if questions remain regarding how the agency should effectuate its goals. This broad-based appreciation for what the Commission seeks to achieve should provide continued momentum for it and all parties to move forward in pursuit of a consensus-based solution.

¹⁹ See, e.g., [Comments of the American Library Association](#), filed June 1, 2018 in WC Docket No. 18-89, at 1 (“ALA Comments”); CTIA Comments at 1; EchoStar/Hughes Comments at 1-2; [Comments of ITTA – The Voice of America’s Broadband Providers](#), filed June 1, 2018 in WC Docket No. 18-89, at 1, 9 (“ITTA Comments”); Motorola Comments at 2; [Comments of Rural Broadband Alliance](#), filed June 1, 2018 in WC Docket No. 18-89, at 3-5 (“RBA Comments”); [Comments of the Satellite Industry Association, Global VSAT Forum, and EMEA Satellite Operators Association](#), filed June 1, 2018 in WC Docket No. 18-89, at 1.

²⁰ [Comments of Puerto Rico Telephone Company, Inc.](#), filed June 1, 2018 in WC Docket No. 18-89, at 1-2 (“PRTC Comments”).

²¹ RBA Comments at 15.

²² [Comments of TracFone Wireless, Inc.](#), filed June 1, 2018 in WC Docket No. 18-89, at 1 (“TracFone Comments”).

²³ CCA Comments at 49.

II. A RULE FOCUSED ON SPECIFIC SUPPLIERS WOULD COMPLEMENT GENERAL SUPPLY CHAIN RISK MANAGEMENT EFFORTS.

Contrary to claims by some commenters, suppliers of concern pose a distinct risk separate and apart from those inherent in the global nature of the supply chain. While frameworks, standards, certifications, and third-party product testing contribute vitally to overall supply chain risk management efforts and bolster ICT networks against myriad vulnerabilities, these tools are not designed to address threats posed by governments with the incentive and ability to exploit the presence of certain entities within the supply chain.

In order to address these threats, both industry and the Commission must rely on the unique national security expertise and intelligence information of the U.S. government. By adopting a targeted rule focused on certain equipment from specific suppliers of concern, the Commission can complement related ongoing supply chain risk management initiatives across industry and the federal government. And by tying its rule to national security determinations made by Congress, the President, or agencies with the requisite expertise, the Commission can support a broader national effort – at once addressing the immediate threat at hand while paving the way for a coordinated interagency effort going forward.

A. Risks Posed by Specific Suppliers of Concern Are Distinct from Inherent Global Supply Chain Risks.

As TIA discussed in its opening comments, this proceeding aims to solve a specific risk posed by certain suppliers' participation in U.S. ICT networks.²⁴ Some commenters suggest that seeking to bar specific suppliers from USF eligibility contradicts the nation's established

²⁴ See TIA Comments at 28-54.

approach to supply chain risk management.²⁵ While TIA, like so many others in this docket, remains firmly committed to a risk management approach to global supply chain security, general supply chain risk management efforts do not address the risks posed by state-sponsored actors with the incentive and ability to conduct cyberespionage or disrupt U.S. networks by exploiting specific suppliers of concern. To mitigate these specific threats, the government must bring its unique resources and intelligence information to bear.

Several commenters argue that the Commission should not act due to the global nature of the supply chain. For example, Huawei points out that “[w]e all rely on a global supply chain and that global supply chain generates potential threats to all countries and companies,” which could be mitigated with “basic cyber hygiene.”²⁶ Indeed, as TIA has noted in other contexts, the global nature of the ICT supply chain presents significant security challenges, which necessitate a collaborative, risk management approach.²⁷ No single government or organization has full authority over the entire network ecosystem, so as a general matter cybersecurity and supply chain risk management rely on frameworks of best practices, standards, and certifications, as well as ongoing partnerships between government and private stakeholders to encourage information sharing and a constantly improving risk posture overall. As detailed in our opening comments, TIA has actively participated in foundational initiatives such as the NIST

²⁵ See CCA Comments at 20-22; [Comments of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc.](#), filed June 1, 2018 in WC Docket No. 18-89, at 49-52 (“Huawei Comments”); ITTA Comments at 1-4; NTCA Comments at 10-13.

²⁶ Huawei Comments, Ex. A, Suffolk Decl. at 1-5.

²⁷ TIA Comments at 29-30 & n.73 (describing how TIA has “champion[ed] policies to facilitate effective approaches to supply chain and cybersecurity risk management through strong collaboration between public and private sectors” and collecting TIA’s filings with DOD, the Commission, NIST, and NTIA).

Cybersecurity Framework, NTIA multistakeholder processes, and Critical Infrastructure Coordinating Councils, among other efforts in support of this approach, and will continue to do so in the years ahead.²⁸

However, Huawei also argues that because supply chains are global, “security risks arise from the cumulative supply chain, *not* the vendor whose name happens to be on the ‘box.’”²⁹ Huawei further asserts that “to achieve the stated objective of the FCC based on the criteria of where something is built, or where components come from, the USA would need to make all of its own ICT components locally or have total control over every global process and supply chain.”³⁰ TIA does not support and does not understand the Commission to be proposing a country-of-origin ban.³¹ Nor does the United States need to manufacture everything locally or assert total control over the supply chain to prevent USF dollars from directly supporting suppliers deemed to pose a threat to national security.³²

To be sure, TIA has acknowledged that it may be important for the Commission to examine issues regarding components in addition to end products in order to better address the national security risk at hand.³³ That said, the heart of the issue is still about which specific suppliers are producing those components or end products. The security risk the Commission seeks to address in this proceeding specifically stems from documented concerns voiced by U.S. intelligence officials, congressional reports, and elsewhere that specific suppliers have ties to

²⁸ *See* TIA Comments at 28-35.

²⁹ Huawei Comments, Ex. A, Suffolk Decl. at 3 (emphasis added).

³⁰ *Id.* at 2.

³¹ TIA Comments at 44-47.

³² *See id.* at Appendix (proposing rule text for a narrowly tailored approach).

³³ *Id.* at 47-53.

foreign governments that make them uniquely susceptible to exploitation to the detriment of U.S. national security.³⁴ This is not a vulnerability that stems from technical, architectural, or organizational deficiencies – which supply chain risk management standards and certifications are best-suited to address – but rather, from a vulnerability based on the supplier itself. Neither industry nor the Commission itself can address this threat on its own, but the Commission can rely on the findings of federal intelligence experts to address this specific threat to programs under its charge.

B. A Rule Focused on Specific Suppliers of Concern Would Not Interfere With General Supply Chain Risk Management Efforts By Government and Industry.

In keeping with its explicit intent to play “an important, supporting role” consistent with its “obligation to be responsible stewards of the public funds used in the Universal Service Fund,” the Commission’s adoption of a targeted rule to address the specific threat posed by certain communications equipment providers would complement industry and government efforts to promote broader supply chain risk management.³⁵ Some commenters argue that the proposed rule would interfere with ongoing initiatives at DHS or DOC.³⁶ However, by adopting a narrowly tailored rule here, the Commission would put a stake in the ground to define its role as complementary to the broader cybersecurity work of the rest of the federal government, deferring to those with appropriate expertise when needed and acting on its own expertise when uniquely positioned to do so.

³⁴ *Id.* at 34-35.

³⁵ Notice ¶ 2.

³⁶ *See, e.g.*, CCA Comments at 20-22.

NTCA argues that the proposed rule would be a “stark departure from the risk-management approach to supply chain security,” as embodied through efforts that include the NIST Cybersecurity Framework and the Communications Security Reliability and Interoperability Council (“CSRIC”) work on this issue.³⁷ However, nothing in the Notice or in the comments supporting it signals a break from the general risk management approach behind which the private sector and the U.S. government have united. Rather, the Notice would initiate a narrow rule that complements, and does not disrupt, that approach. As discussed in section II-A above, the proposal does not address supply chain risk management generally; instead, it pertains specifically to suppliers whose (1) close relationships with state actors with sophisticated and aggressive cyber espionage capabilities and/or (2) past misconduct or illegal activity give rise to articulable national security concerns that are distinct from the general supply chain risk management concerns that apply to other suppliers of similar equipment and services.

Parties that oppose Commission action appear to lose perspective on the scope of that potential action. Far from contemplating some sort of far-reaching new regulatory regime that would supplant the risk-based approach that prevails today, the Commission is simply considering a narrowly tailored restriction on specific suppliers for specific reasons that are reimbursed by Commission-managed funds. Prescriptive regulations such as mandated security products or rules regarding how code is written and verified or how passwords and access controls within a manufacturer’s corporate systems are administered, mandatory audit procedures, or the like are simply not on the table in this proceeding. TIA would not support such measures, and the Commission does not propose any in the Notice.

³⁷ NTCA Comments at 10; *see also id.* at 10-13.

If anything, a narrow rule in this context will facilitate future risk management efforts by further informing ICT companies' assessment of their vulnerabilities and by enhancing coordination within the federal government. As TIA underscored in its opening comments, the Commission takes a targeted view to act within the scope of its own program, while providing the first public opportunity for stakeholders to comment on these issues. The Notice signals the Commission's own risk management process – identifying a risk that it faces, evaluating the extent to which it is willing to accept that risk, and then taking steps to mitigate that risk.

C. A Rule Tied to Determinations Made by the Executive Branch or Congress Regarding Specific Suppliers Would Contribute to a Broader National Effort.

Commenters, including TIA, overwhelmingly agree that DHS, in coordination with DOC and others, is well-positioned to lead broader national efforts on supply chain security.³⁸ However, some commenters argue that action by the Commission to address suppliers of concern within the USF program could disrupt broader efforts by other agencies allegedly better suited to act on these issues.³⁹ Others argue the Commission should wait for a broader national strategy to lead the way.⁴⁰ While TIA agrees that the federal government should pursue a coordinated national strategy to address supply chain security, we see no reason why targeted action by the Commission would interfere with ongoing supply chain security initiatives within DHS, DOC, or elsewhere. On the contrary, a narrowly tailored rule would support an ongoing national effort to protect U.S. ICT infrastructure. By adopting a rule tied to determinations made by branches of the government with appropriate national security authority, the Commission can both address

³⁸ See *supra* section I-A & nn.10-12.

³⁹ See CCA Comments at 20-22; NTCA Comments at 13.

⁴⁰ PRTC Comments at 6.

the pressing issue at hand, while leaving room for a coordinated interagency process going forward.⁴¹

By acting within its intended scope, the Commission can support national security efforts in an area over which the Commission has distinct authority. CCA points to ongoing DHS assessments of supply chain security risks and the DOC denial order regarding ZTE, concluding that “[i]t is more appropriate for DHS, rather than the FCC, to *take the lead* on issues pertaining to the national supply chain and national security.”⁴² We agree with CCA that appropriate security agencies like DHS (or Congress) should *take the lead* on issues regarding specific suppliers of concern, but we also agree with the Commission that it has a “specific, but important, *supporting role* to play in these efforts.”⁴³ Taking steps to ensure that USF dollars do not go to suppliers posing a national security threat is uniquely within the Commission’s purview, as the Commission bears the distinct responsibility of overseeing the program. Though this proceeding may inform a broader discussion, the Commission’s actions to bar these specific suppliers from USF reimbursement – if properly tailored – would involve the Commission implementing national security determinations made by Congress or expert agencies, not the Commission taking the lead on cybersecurity strategy writ large.

As anticipated by the Commission, a rule tied to national security determinations made by Congress or the Executive Branch would complement related ongoing initiatives in other federal agencies. NTCA claims that the Notice “lacks broader discussion of how the FCC’s potential actions tie to the simultaneous actions of other Federal agencies and the Executive

⁴¹ TIA Comments at 54-60 & Appendix.

⁴² CCA Comments at 20-22; *id.* at 22 (emphasis added).

⁴³ Notice ¶ 2 (emphasis added).

branch administration,” observing that DHS is the sector-specific agency assigned to the information and communications industries.⁴⁴ NTCA additionally describes the DOC action on ZTE and proposals in Congress on supply chain security, concluding that it is unclear how the Commission’s proposal here “ties to the many ‘irons in the fire’” regarding supply chain threats.⁴⁵ TIA agrees with NTCA that any Commission action on national security grounds that is not “tied” to actions by others in the government with appropriate insight and expertise would be problematic. Precisely for that reason, TIA has urged the Commission to adopt a rule that explicitly ties its own list of prohibited suppliers to determinations already made by agencies with appropriate expertise or by Congress.⁴⁶ Contrary to NTCA’s suggestion, the Commission has also discussed this potential relationship in the Notice.⁴⁷ If anything, by adopting this Notice, the Commission has already enhanced coordination with other federal agencies on this topic and received valuable input on related initiatives of which to be mindful.⁴⁸

Given the nature of the risk the Commission aims to address, the targeted manner in which it proposes to proceed, and the unique position the Commission has with respect to the USF, we see no reason for the Commission to delay moving forward. Puerto Rico Telephone Company suggests that the Commission should “defer action on the proposed rule” and wait for the development of a comprehensive government strategy to address ICT supply chain risks.⁴⁹

⁴⁴ NTCA Comments at 13.

⁴⁵ *Id.* at 14-15.

⁴⁶ TIA Comments at 54-60.

⁴⁷ Notice ¶¶ 20-23.

⁴⁸ *See, e.g.*, Letter to Marlene Dortch, Secretary, FCC, from Mike Saperstein, USTelecom, WC Docket No. 18-89, at 1 (filed May 25, 2018) (noting that discussions very closely related to the issues set forth in the Notice are currently taking place at DHS, DOC, and in Congress).

⁴⁹ PRTC Comments at 6.

While TIA agrees with commenters who advocate a coordinated national strategy, we see no persuasive argument that the Commission should wait to act on a national security threat for a broader strategy with no specified timeline that may not address the specific question at issue. By adopting a rule tied to determinations made by Congress and the Executive Branch, the Commission can take steps to address a timely issue while paving the way for a coordinated interagency process going forward.

D. Supply Chain Standards and Certifications Are Not Designed to Address Risks Presented by Specific Suppliers Connected to Sophisticated State-Sponsored Actors.

As discussed in TIA’s opening comments and supported by the vast majority of commenters in this proceeding, the Commission itself is not in a position to determine what does and does not present a threat to national security.⁵⁰ In adopting a narrowly tailored rule to prevent the USF from supporting suppliers that present a threat to national security, the Commission must rely on designations made by others in the federal government with the appropriate insight and expertise to make that determination. Therefore, it would be inappropriate for the Commission to evaluate whether use of an industry standard or obtaining an industry certification negates a national security threat identified by the U.S. federal government.

That said, several commenters point to such frameworks, standards, and certifications as evidence of why the Commission need not take action to address USF-funded suppliers whose presence in the supply chain is deemed to pose a threat to national security. For example, Huawei notes it “has achieved many international certifications from many standards and certification bodies including for ISO standards, counter terrorism protection in supply chain,

⁵⁰ TIA Comments at 59-60; *see supra* section I-A.

cloud operations, TQM for Six Sigma and TL9000, product standards such as FIPS for encryption and common criteria for products.”⁵¹ Huawei additionally details participation in third-party product testing.⁵² While TIA ultimately defers to appropriate experts within the U.S. government to determine what constitutes a national security threat, we discuss below why these risk management tools do not address the problem at hand.

Frameworks, standards, and certifications are vital to supply chain security as part of a holistic risk management approach; however, these tools are not designed to address threats posed by specific suppliers with close ties to foreign governments with the incentive and ability to exploit the presence of certain entities in the ICT supply chain. Most of the security programs identified by commenters provide tools for entities to manage their own cyber, physical, or information security risks and communicate their risk management posture to others. For example, the NIST Cybersecurity Framework is designed as a set of voluntary tools to help enterprises assess and manage their cybersecurity risks, while – through increasing use – providing an international, ubiquitous language for communicating cybersecurity risk management.⁵³ Even more broadly, the Total Quality Management (“TQM”) for Six Sigma provides a “method for organizational management that focuses on improving the quality of services and products produced ... by providing ongoing improvements based on feedback.”⁵⁴

While use of these tools certainly can contribute to a better risk posture as an organization, such

⁵¹ Huawei Comments, Ex. A, Suffolk Decl. at 8.

⁵² *Id.*, Ex. B, Purdy Decl. at 33-41.

⁵³ See NIST, *Cybersecurity Framework*, <https://www.nist.gov/cyberframework> (visited June 29, 2018).

⁵⁴ Six Sigma, “Achieve Business Excellence with Total Quality Management (TQM)” (Feb. 21, 2017), <https://www.6sigma.us/six-sigma-articles/achieve-business-excellence-with-tqm/>.

use by no means prevents a foreign government from exploiting unique influence within an organization's access to its own products.

Likewise, industry standards provide valuable arenas for industry and stakeholders to agree on important sets of process guidelines or minimum requirements to address specific technical or organizational vulnerabilities in developing products, while certifications provide a means of communicating conformity to a specific standard. The ISO/IEC 20243 Open Trusted Technology Provider Standard (“O-TTPS”), for example, “provides a set of guidelines, requirements, and recommendations that help assure against maliciously tainted and counterfeit products throughout the [commercial-off-the-shelf] COTS ICT product life cycle” throughout the “design, sourcing, build, fulfillment, distribution, sustainment, and disposal” phases as well as “assessment procedures that may be used to demonstrate conformance” with the specified requirements.⁵⁵ As another example, ISO/IEC 27036-3:2013 provides “guidance to ICT product and service acquirers and suppliers to reduce or manage information security risk” by identifying “the business case for ICT supply chain security, specific risks and relationship types as well as how to develop an organizational capability to manage information security aspects and incorporate a lifecycle approach to manage risks supported by specific controls and practices.”⁵⁶ TIA’s own TL9000 program provides, among other elements, a benchmarking service to measure an organization’s individual performance against aggregate best-in-class, average, and

⁵⁵ ISO/IEC, *Information technology – Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products*, 20243-1, at vi (2018), http://standards.iso.org/ittf/PubliclyAvailableStandards/c074399_ISO_IEC_20243-1_2018.zip (emphasis added).

⁵⁶ ISO/IEC, *Information technology – Security techniques – Information security for supplier relationships – Guidelines for information and communication technology supply chain security*, 27036-3 (2013), <https://www.iso.org/obp/ui/#iso:std:iso-iec:27036:-3:ed-1:v1:en>.

low bar rating of aggregated participant data – a way to compete against others in the market for customer satisfaction.⁵⁷ However, such programs do not provide methods to communicate a lack of influence within an organization by a foreign government.

Some commenters point to third-party testing and evaluation as a way to ensure the security of supplier products.⁵⁸ As the 2012 HPSCI Report explained, “[p]rocess like the Common Criteria for Information Technology Security Evaluation and various private certification services define a process by which an evaluator measures a product against a set of standards and assigns a security rating ... to help a consumer know how much confidence to place in the security features of the device or software package.”⁵⁹ However, “such processes are not necessarily designed to uncover malicious code but to encourage a foundational security baseline in security-enabled products.”⁶⁰ As TIA has explained, constructing a testing regime to detect whether a communications technology product has been deliberately and covertly

⁵⁷ See generally TL 9000, *TL 9000 Benchmark and Performance Data*, <http://www.tl9000.org/registration/pdrs.html> (visited June 29, 2018). TL 9000 is managed by QuEST Forum, an organization that merged with TIA in 2017. Press Release, QuEST Forum, *TIA and QuEST Forum Announce Merger*, Sept. 19, 2017, <https://www.questforum.org/tia-and-quest-forum-announce-merger/> (visited July 2, 2018).

⁵⁸ See Huawei Comments, Ex. A, Suffolk Decl. at 9 (noting Huawei uses and “customers are free to adopt any verification method they wish, a wide range of security testing companies from the USA, Europe and Asia to validate our products”); see also *id.*, Ex. B, Purdy Decl. at 36 (discussing Huawei’s participation in the EWA North America security evaluations and Trusted Delivery program, including “in-depth analysis of source code and resulting binaries, including design and actual available functionality; firmware; and an array of system-level testing processes executed in both EWA NA and carrier laboratory environments”).

⁵⁹ Permanent Select Committee on Intelligence, U.S. House of Representatives, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, at 5 (Oct. 8, 2012) (“HPSCI Report”), [https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huaweizte%20investigative%20report%20\(final\).pdf](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huaweizte%20investigative%20report%20(final).pdf).

⁶⁰ *Id.*

compromised by a state-sponsored actor seeking to commit cyberespionage presents unique, if not insurmountable, challenges. Product testing – no matter how rigorous or well-designed – is insufficient to address concerns from such products.⁶¹ Flaws deliberately and covertly introduced into a chipset design find easy hiding places in the complexity of modern circuitry, and while a third-party program can test a “statistically significant” number of products, it cannot feasibly test every product. At the software layer, even if given the source-code, a third-party laboratory cannot reliably prevent carefully-hidden exploits from slipping through the cracks.⁶²

While industry security standards, certifications, and third-party testing play important roles in general supply chain security risk management, they do not negate the validity of the Commission’s role in protecting USF networks. These tools are invaluable in helping organizations address some problems, but they do not solve every security problem.

III. THE BENEFITS OF A NARROWLY TAILORED USF RESTRICTION WOULD FAR OUTWEIGH ANY POTENTIAL COSTS.

Not a single commenter questions – nor could they – the benefits of ensuring the security of communications equipment and networks supported by universal service dollars. It is unchallengeable that individual consumers, businesses, schools, libraries, and health care providers will benefit from a policy that protects them – and those they interconnect with – from purchasing equipment or services from companies that have been identified as posing a substantial cybersecurity risk and who threaten U.S. national security. To suggest otherwise would strain credulity. These benefits must of course not be outweighed by potential costs to the

⁶¹ TIA Comments at 36-38.

⁶² *See, e.g., id.* at 37 n.92 (detailing how the Multi-State Lottery Association information-security director rigged the outcome of the national Hot Lotto game); *id.* at 38 n.94 (noting that the source code had been certified by a major testing lab after the lab had performed an audit of the source code).

Commission's universal service programs and those supported by them. Notwithstanding the doomsday scenarios suggested by select commenters, based on the exceedingly few entities that appear to presently purchase equipment or services from Huawei or ZTE using USF dollars, and the highly competitive market for all equipment and services that they provide, it is clear that the benefits of the Commission's proposal vastly outweigh any potential harms.

A handful of comments, primarily those of Huawei and to a lesser extent CCA, suggest that Huawei and ZTE do not in fact pose a cybersecurity risk, thereby attempting to strip the Commission of any purported benefits of preventing USF dollars from being spent on Huawei or ZTE equipment.⁶³ TIA agrees that a determination as to whether a company is a national security risk is not a decision for the FCC to make,⁶⁴ but TIA has demonstrated that such a decision has quite clearly already been made by the relevant expert agencies with respect to Huawei and ZTE.⁶⁵ Thus, there are clear and recognizable benefits to the FCC protecting the interests of USF recipients by ensuring the security of USF-supported equipment and networks.

In addition to challenging the need for a rule, opponents attempt to call into question the ability of the Commission to achieve its universal service objectives if certain companies are excluded from the program. Such commenters seek to paint a dire picture suggesting that the broad deployment of networks in rural areas can only occur using equipment from the problematic suppliers, and without this equipment, significantly less deployment will occur. These same arguments are the basis for a claim that the FCC's proposal is inconsistent with the

⁶³ See CCA Comments at 34, 37-40; Huawei Comments at 54-55, 86-91.

⁶⁴ See TIA Comments 27, 58-60; see also CTIA Comments at 18; Huawei Comments at 19; ITTA Comments at 3-4.

⁶⁵ TIA Comments at 10-18.

universal principles found in Section 254(b) of the Communications Act, an easily rebuttable claim once the rhetoric is separated from the facts.⁶⁶ The reality is that the vast majority of entities who have received USF support to date to serve rural America have successfully met their USF obligations, providing quality service (including advanced services) that are reasonably comparable to services provided to urban Americans and offered at reasonably comparable rates, without reliance on Huawei or ZTE. That has been true and will be true even if the Commission prohibits USF support from being spent on equipment from these companies.

TIA is, however, sympathetic to the arguments concerning the costs that may be incurred by companies that have used USF funds to purchase equipment from Huawei or ZTE when such purchases were made consistent with program rules at the time. Therefore, TIA supports consideration of remedial measures that might be taken to address legitimate costs incurred by such companies.⁶⁷ However, potential harms to a small number of rural wireless carriers is not a sufficient justification for rejecting a critically important universal service policy. As TIA stated in its initial comments in describing the FCC’s responsibility for balancing the competing considerations of any given USF policy choice, “when it comes to national security, there is less room – and perhaps no room – for tradeoffs.”⁶⁸ Nothing in the record suggests otherwise.

A. A Narrowly Targeted Rule Would Provide Important Cybersecurity Benefits to USF Beneficiaries While Making a Meaningful Contribution to National Security.

A narrowly tailored rule, as TIA explained in its opening comments, would significantly reduce the risk posed by certain suppliers’ participation in the ICT supply chain to both USF-

⁶⁶ See *infra* section V-A.

⁶⁷ See *infra* section III-D.

⁶⁸ TIA Comments at 65.

funded networks and those that interconnect with them.⁶⁹ As USTelecom articulates, “[T]here is a substantial body of evidence suggesting that risks to the confidentiality, integrity, and authenticity of the nation’s communications networks emanate from the use of certain providers of network equipment and services, including Huawei, ZTE, and Kaspersky Labs.”⁷⁰ While the networks of USF-funded entities alone are vital enough to deserve protection from national security threats, as commenters note, the USF “funds networks in every state, territory, and tribal region of the United States,”⁷¹ And these networks interconnect indiscriminately with commercial broadband networks across the country and internationally. By doing its part to protect USF recipients, the Commission can help make the ecosystem safer for everyone, an objective broadly shared by commenters as described in section I-B above.

Moreover, there is no doubt, as TIA explained in its initial comments, that there are national security benefits from ensuring the security of broadband networks and equipment used by schools, libraries, and health care providers.⁷² To that end, the State E-Rate Coordinators Alliance “acknowledges and applauds the Commission’s concern” over the integrity of USF-funded equipment and services, agreeing that special consideration needs to be given to schools and libraries (and rural health care providers) ““which may not be as well-positioned as a carrier receiving USF support to know whether the services and/or equipment they purchase with USF support are being provided by an entity that poses a supply chain integrity risk.””⁷³ The

⁶⁹ *Id.* at 66-71.

⁷⁰ USTelecom Comments at 3.

⁷¹ Motorola Comments at 3.

⁷² TIA Comments at 6-7.

⁷³ [Comments of the State E-Rate Coordinators Alliance](#), filed May 29, 2018 in WC Docket No. 18-89, at 2 (quoting Notice ¶ 17) (“SECA Comments”).

American Library Association concurs, stating that it agrees with the Commission’s proposal that “no Universal Service Funds (USF) should be ‘used to purchase or obtain any equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain.’”⁷⁴

By carefully tailoring its rules to fully address the presence of suppliers of concern in the USF supply chain, the Commission can address the specific parts of the supply chain that pose an actual national security threat. Huawei’s expert consultant on cybersecurity argues that if the Commission adopts the proposed rule, “any benefits to national security would be marginal, and likely insignificant.”⁷⁵ The consultant asserts that the impact of the Commission’s action would be ineffective because the proposed rule focuses only on final sellers of equipment and does not address threats arising from components nor does it consider the specific nature of the final product.⁷⁶

However, as TIA has discussed at length, the problem the Commission seeks to address in this proceeding is rooted in the identity of specific suppliers and the unique threat they pose to the USF ICT supply chain. This proceeding does not seek to address every cyber and physical security risk in the ICT supply chain and does not need to address every risk in order to make a meaningful impact. That said, TIA agrees that tailoring the proposed rule to account for *components* from suppliers of concern could help target the rule more effectively and make a more *meaningful* contribution to national security.⁷⁷ To that end, TIA has proposed a definition

⁷⁴ ALA Comments at 1 (quoting Notice ¶ 16).

⁷⁵ Huawei Comments, Ex. G, Tow Decl. ¶ 4.

⁷⁶ *Id.* ¶¶ 4, 10-11, 14.

⁷⁷ TIA Comments at 47-53.

of “logic-enabled components” for consideration by the Commission and by other commenters.⁷⁸ Likewise, TIA agrees that certain low-level communications products like physical enclosures pose less security risk, so restrictions on end products could appropriately be limited to those products from suppliers of concern that contain a logic-enabled component.⁷⁹ If a supplier of concern wishes to sell physical enclosures or similar products that pose no real threat to USF recipients, there are any number of ways the Commission’s final rule could enable that.⁸⁰

By adopting a narrowly tailored rule, the Commission can significantly diminish the threat faced by USF recipients and those that interconnect with them. Huawei’s expert argues that USF recipients are “not the likely targets of attack” by a hostile government or other actor because small or rural carriers, school districts, public libraries, and rural health care providers are “not the high-value targets that a foreign government or its agents would be likely to target

⁷⁸ *Id.* at 88-89. Issues regarding components remain in flux, with the Senate recently taking yet another approach to intelligent components in its version of the FY19 NDAA. *See* H.R. 5515 § 6702(e)(1), 115th Cong. (printed as passed by the Senate, June 19, 2018). Meanwhile, even “passive” or “dumb” components could potentially tap either electrical or optical signals and gain unauthorized access to the data being transmitted, although some form of physical proximity to the compromised device would likely be needed to effectuate any actual interception. For example, optical splitters can be used on a fiber optic cable to tap off a small amount of optical power (*e.g.*, 5 percent, 2 percent, or even less than 1 percent) and route the signal to a different destination or listening device. Antennas could be utilized in a similar way. The equipment can be designed to behave in this way without needing to be tampered with later or installed in a specific manner, although the physical proximity requirement – *i.e.*, installing another listening or other device to retransmit the intercepted data, or having an agent on the ground – renders such threats to be somewhat qualitatively different in nature *vs.* that presented by remote hacking that exploits “logical” backdoors. Regardless, TIA remains open to further engagement with other stakeholders on this matter.

⁷⁹ *See* TIA Comments at 47-48 (noting that different types of components have different impacts on security, for example, the “potential security impact of a network interface card or a CPU is quite different from that of a plastic housing or a screw, or even from that of low-level electronic components like capacitors, resistors, or op-amps”).

⁸⁰ *See* TIA Comments at Appendix for one example.

with a cyberattack or disruption of supply.”⁸¹ Such a conclusory statement is unsubstantiated given that Huawei’s expert cannot presume to know a foreign government’s long-term plans for espionage, information operations, or strategy. In addition, rural areas served by these USF-funded providers could include sensitive installations, such as military bases.

In fact, current trends suggest that USF-funded networks may be among those most acutely targeted – as explained in TIA’s opening comments, health care providers in particular are experiencing a rapid increase in cybersecurity attacks at far greater levels than other industries.⁸² Furthermore, malicious disruption in the network may be motivated by any number of reasons and hackers tend to exploit the easiest avenues available to them. While one might surmise there are more significant targets for a nation-state to attack than others, there is no basis to suggest that the underserved communities, schools, libraries, and hospitals that benefit from USF funding are safe. Regardless, these networks interconnect indiscriminately with commercial networks all over the United States. If suppliers (or their equipment or components) pose a threat to some entities in the network, they pose a threat to everyone in the network.

Finally, by adopting a tailored rule, the Commission can make a meaningful impact on national security within the scope of the part of the ecosystem over which it has authority, working symbiotically with other agencies with relevant expertise and jurisdiction. Huawei’s expert argues that the proposed rule ignores post-production logistics and supply chain risks, observing that potential threats could be introduced at “consolidation, border crossings, storage & distribution and last mile transport.”⁸³ Even if true, such risks are of a different nature than

⁸¹ Huawei Comments, Ex. G, Tow Decl. ¶¶ 4, 13.

⁸² TIA Comments at 7.

⁸³ Huawei Comments, Ex. G, Tow Decl. ¶¶ 4, 12.

those the Commission proposes to address, because they may require physical access to the equipment in the United States, unlike hardware or software backdoors that could be introduced overseas during the design or development stage. In any event, the Commission is not required to address every threat vector in this proceeding,⁸⁴ and the different nature of such post-production threats provides ample basis to justify not considering them in this proceeding. Ultimately, as the vast majority of commenters affirm, the Commission should rely on the national security expertise of those in the federal government with the insight and authority to make such determinations, with the FCC playing an important but limited role within the greater cybersecurity risk management ecosystem.

As nearly every commenter in this docket explains, cybersecurity, particularly as it relates to the ICT supply chain, is a complex endeavor in which each participant in the network ecosystem must assess risks faced, determine the level to which each risk is acceptable or unacceptable, and manage those risks accordingly. This is an ongoing process that requires participants to evaluate and reevaluate over time using the best data available to take what steps are within the scope of its control to make meaningful improvements. In adopting the Notice, the Commission is doing just that.

B. The Number of Affected Carriers Would Potentially Be Very Small and the Costs Would Be More Limited Than Certain Commenters Suggest.

As noted in our initial comments, TIA is not aware of any publicly-available data regarding the number of USF recipients that currently use Huawei or ZTE equipment in their infrastructure.⁸⁵ However, information obtained by TIA indicates that there are currently thirteen

⁸⁴ See section V-B-2.

⁸⁵ TIA Comments at 71.

U.S. wireless carriers, all of which are small and/or rural carriers that receive USF support, that use either Huawei or ZTE equipment as a substantial part of their wireless network infrastructure.⁸⁶ Of these, it appears that eleven use Huawei equipment while two use ZTE equipment,⁸⁷ and that nine of these deployments are wireless mobile access while the other four are predominantly fixed wireless deployments.⁸⁸

The wireless mobile access deployments represent approximately 1,300 cell sites in total, and all of the wireless deployments including primarily fixed wireless deployments represent less than 1,500 sites in total.⁸⁹ Since there are approximately 300,000 cell sites in the United States, Huawei and ZTE's combined share of the U.S. wireless infrastructure market appears to therefore be approximately *one half of one percent or less*.⁹⁰ Although there may be some wireless carriers not reflected in the information obtained by TIA, there is good reason to believe that this data reflects a reasonably complete picture because all seven of the carriers that filed declarations attached to CCA's initial comments were represented in the data:

- SI Wireless LLC d/b/a MobileNation
- NE Colorado Cellular d/b/a Viaero Wireless
- James Valley Telecommunications
- United Telephone Association, Inc.
- Nemont Telephone Cooperative, Inc. / Sagebrush Cellular, Inc.

⁸⁶ See Appendix *infra*, Declaration of Cinnamon Rogers ¶ 6 (“Rogers Decl.”).

⁸⁷ *Id.*

⁸⁸ *Id.* ¶ 6(a). TIA also believes there may be two wireless internet service providers (“WISPs”) that use Huawei or ZTE equipment to deliver service using proprietary or Wi-Fi-based technologies that are distinct from the current-era fixed wireless LTE services included above.

⁸⁹ *Id.* ¶ 6(b).

⁹⁰ *Id.* ¶ 6(c); see also *Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services*, Twentieth Report, 31 FCC Rcd 10534 ¶ 43 (2017) (citing CTIA data that there were 308,334 cell sites in use at year-end 2016) (“*Twentieth Mobile Competition Report*”); TIA Comments at 71 (citing news report indicating that Huawei's U.S. market share is less than one percent).

- Pine Belt Cellular, Inc.
- Union Telephone Company d/b/a Union Wireless⁹¹

While it is likely that the data obtained by TIA provides a reasonably complete picture of USF-supported wireless carriers that receive USF support, there may also be wireline carriers that use Huawei and/or ZTE equipment. Data provided to TIA does not address that market segment, and these reply comments are focused on responding to the comments filed in response to the Notice, the predominant focus of which was on the impact to rural wireless carriers. Further, these numbers do not reflect the possibility that private non-USF-funded networks may also use Huawei or ZTE products, but that is beyond the scope of the current proceeding.

The cost estimates for replacement provided by potentially affected carriers – as much as \$410 million for one carrier alone⁹² – appear to be unrealistically high. Of course, specific prices for wireless equipment would vary significantly depending upon the technology used and commercial arrangements involved. However, information obtained by TIA indicates that a price of \$100,000 per site is a reasonable upper-end estimate for the costs of wireless cell site equipment.⁹³ Information from anecdotal and public sources confirms that a rough order-of-magnitude calculation based on a price of \$100,000 per site for wireless equipment – which may

⁹¹ Rogers Decl. ¶ 7; *see also* CCA Comments at 6, Beehn Decl., DiRico Decl., Groft Decl., Houseman Decl., Kilgore Decl., Nettles Decl., Woody Decl.

⁹² *See* CCA Comments, DiRico Decl. ¶ 4.

⁹³ Rogers Decl. ¶ 8 (also noting that costs “would likely be significantly less” than \$100,000 per site).

actually be quite high – would be reasonable.⁹⁴ Using that figure, the total cost of equipment to replace Huawei and ZTE wireless infrastructure equipment in *all* affected carriers would be on the order of 1,500 sites x \$100,000 per site = \$150 million,⁹⁵ plus legitimate installation costs.

C. USF Recipients Will Continue to Benefit from a Competitive Vendor Market.

In our opening comments, TIA provided extensive detail regarding the equipment marketplace.⁹⁶ In contrast, for the most part, opponents of Commission action generally rely on anecdotes and speculation. CCA asserts that “[t]he proposed rule will reduce the number of suppliers of *core* network equipment from five to three,” with the unexplained caveat that “[t]here are additional providers of discrete network components.”⁹⁷ Notably, CCA does not elaborate as to when or why any specific equipment would be considered “core” or not. A Huawei official goes further, claiming that “[t]he U.S. infrastructure market ... is dominated by

⁹⁴ There is significant variation in public sources regarding equipment pricing, including a lack of clarity regarding whether particular cost estimates refer to wireless equipment costs only or to combined tower construction costs as well. However, the information suggests that an average price of \$100,000 per site for equipment alone would likely be on the higher end of the range. *See, e.g.*, Federal Communications Commission, *A Broadband Network Cost Model: A Basis for Public Funding Essential to Bringing Nationwide Interoperable Communications to America’s First Responders*, May 2010, at 9, <https://transition.fcc.gov/national-broadband-plan/broadband-network-cost-model-paper.pdf> (assumption of \$95,000 blended average per site capex for adding public safety broadband to commercial LTE cell site); *id.* at 13-14 (showing total equipment costs of approx. \$70,000 before installation); Chris LaPeters, *How Much Does LTE 4G Radio Base Station Cost*, QUORA, Aug. 4, 2016, <https://www.quora.com/How-much-does-LTE-4G-radio-base-station-cost> (“In my experience, the typical Ericsson eNodeB with 3 radios ... will run about 60K +/-.”).

⁹⁵ Rogers Decl. ¶ 8.

⁹⁶ *See* TIA Comments at 72-77.

⁹⁷ CCA Comments at 37 & n.80 (emphasis added).

only *two* major telecom equipment suppliers.”⁹⁸ Likewise, WTA’s claim that the market has gone from five to two suppliers is based on a single anecdote offered by one carrier.⁹⁹

As shown in TIA’s opening comments, these statements are clearly erroneous, as there are far more than three – let alone two – major telecommunications equipment suppliers selling into the U.S. market.¹⁰⁰ As best as TIA can discern, commenters who express concerns about even the impact of a narrowly tailored rule focused on USF funding *might* be focusing solely on the market for *wireless radio access equipment*. While that is an important market segment, it forms only one portion of the equipment necessary to deploy a mobile network. As shown below, all aspects of the marketplace – including “core,” wireline, and wireless access – are robustly competitive.

1. USF Recipients Have Many Options for Core Equipment, Wireless and Wireline Access Equipment, End-to-End Network Design and Installation Services, and Support Services.

The general architecture of networks from basic telephony through the Internet is that wired and wireless *access* networks connect end users to the global network by routing traffic back through the provider’s core network, while “core” equipment and functions such as routing and switching are typically wired and use optical connections. Of course, fixed-wireless backhaul applications, particularly in rural areas, arguably constitute a middle ground – and middle-mile – between “core” routers and switches in a central office and “access” networks

⁹⁸ Huawei Comments, Ex. C, Dowding Decl. ¶ 25.

⁹⁹ [Comments of WTA – Advocates for Rural Broadband](#), filed June 1, 2018 in WC Docket No. 18-89, at 4-5 (“WTA Comments”).

¹⁰⁰ *See, e.g.*, TIA Comments at 74 & n.161 (mentioning ADTRAN, Cisco, Ericsson, Fujitsu, Juniper Networks, Nokia, Ribbon Communications, Samsung, and Tellabs).

serving end customers.¹⁰¹ Regardless, the *wireline* equipment market therefore remains vitally important to every service provider. Importantly, a particular device used as a “core” router or switch by a small service provider may often be configured as an “edge” or “access” device by larger providers, even as various ICT manufacturers may market their specific products as “core” or “edge” products that run the gamut from small to large applications.

Core and/or wireline equipment. As TIA explained in our opening comments, there are many manufacturers and suppliers of wireline networking equipment.¹⁰² Manufacturers like ADTRAN, Arris, Calix, Casa, Cisco, Fujitsu, Infinera, Juniper, Nokia, Ribbon, Samsung, Tellabs, and likely many more produce such products in a wide variety of models and specifications.¹⁰³ In addition to carrier-grade “core” routers and switches, these include wireline access networking products for optical, copper-based, or coaxial cable networking – an important offering, since many USF recipients continue to purchase and deploy various wireline access technologies including DSL, cable modem, and fiber-to-the-home.

¹⁰¹ See, e.g., Fujitsu, *FRX-3 Series Long-Haul Microwave Radio Systems*, <http://www.fujitsu.com/us/products/network/products/frx-3e-long-haul-microwave-radio-system/index.html> (visited June 20, 2018); Nokia, *FastMile –Wireless Broadband Connectivity that Goes Everywhere*, <https://networks.nokia.com/solutions/fastmile> (visited June 25, 2018).

¹⁰² See TIA Comments at 73-76.

¹⁰³ See *id.* at 74 n.161 (collecting links to product portfolios from, *inter alia*, ADTRAN, Cisco, Juniper, Nokia, Ribbon, Samsung, and Tellabs); see also Arris, *Products*, <http://www.arris.com/products/> (visited June 19, 2018); Casa Systems, *All Products*, <http://www.casa-systems.com/all-products.html> (visited June 19, 2018); Calix, *Calix Solutions for Service Providers*, <https://www.calix.com/solutions/service-providers.html> (visited June 19, 2018); Fujitsu Network Communications, *Products*, <http://www.fujitsu.com/us/products/network/products/index.html> (visited June 19, 2018); Infinera, *Mobile Transport*, <https://www.infinera.com/applications/mobile-transport/> (visited June 19, 2018).

In addition to use in “core” functionality and in wireline access deployments, wireline devices also form a large component of any wireless access network deployment, since any wireless network infrastructure necessarily depends on backhaul to connect data traffic from a cellular base station back to a carrier’s “core” network. Optical wireline equipment is also increasingly important for so-called “fronthaul” applications in which a traditional cellular base station is separated into the cell tower itself (radio head) and the mobile network control backbone (baseband unit).¹⁰⁴ For that reason, nearly all of the vendors identified above specifically market their products and solutions to mobile service providers, and their product

¹⁰⁴ See generally Bob DiFazio, Vice President, Future Wireless, InterDigital Labs, *The Fusion of Fronthaul and Backhaul: What it Means for 5G*, RCR WIRELESS, Nov. 15, 2016, <https://www.rcrwireless.com/20161115/sponsored/fusion-fronthaul-backhaul-means-5g>; Eero Ryytty, Nokia, *IEEE802.1CM Terminology Considerations*, Nov. 11, 2015 (discussing definitions of fronthaul, radio equipment controller, remote radio head, baseband unit, etc.) <http://www.ieee802.org/1/files/public/docs2015/cm-rytty-terminologyconsiderations-1115.pdf>; Ericsson, *Mobile Networks: Transport Impacts*, Sept. 2014, at 3 (chart showing role of fronthaul, midhaul, and backhaul), <http://www.ieee802.org/1/files/public/docs2014/new-irvine-mobile-networks-fronthaul-0914.pdf>.

offerings are often specifically tailored with wireless backhaul, fronthaul, or other mobile access applications in mind.¹⁰⁵

Wireless access equipment. Aside from well-known players such as Ericsson, Nokia, and Samsung that have significant shares of the traditional macrocell base station infrastructure market, there are a number of smaller or startup providers ready to compete with incumbents as explained in TIA's opening comments.¹⁰⁶ Many companies also offer wireless radio access network infrastructure products more generally, especially small cell and/or metro cell technologies that are important for 4G and 5G networks, including large companies like Cisco,

¹⁰⁵ See, e.g., ADTRAN, *Mobile Backhaul*, <http://adtran.com/web/page/portal/Adtran/group/482> (visited June 19, 2018); Calix, *Calix Solutions: Mobile Network Operators*, <https://www.calix.com/solutions/service-providers/wireless.html> (visited June 19, 2018); Casa Systems, *Mobile Service Providers*, <http://www.casa-systems.com/solutions-mobile.html> (visited June 19, 2018) (discussing "mobile core evolution to 5G"); Cisco, *Mobile Internet*, <https://www.cisco.com/c/en/us/solutions/service-provider/mobile-internet/index.html> (visited June 19, 2018); Fujitsu, *Mobile Backhaul*, <http://www.fujitsu.com/us/products/network/applications/mobile-backhaul/index.html> (visited June 19, 2018); Infinera, *Mobile Transport*, <https://www.infinera.com/applications/mobile-transport/> (visited June 19, 2018); Juniper, *5G Mobile Network Deployments*, <https://www.juniper.net/us/en/solutions/mobile-provider/> (visited June 19, 2018); Nokia, *5G Anyhaul for Mobile Transport*, <https://networks.nokia.com/solutions/mobile-transport> (visited June 19, 2018); Ribbon Communications, *Mobile Network Solutions*, <https://ribboncommunications.com/solutions/service-provider-solutions/mobile-network-solutions> (visited June 19, 2018); Samsung, *Mobile Packet Core*, <https://www.samsung.com/global/business/networks/core-networks/mobile-packet-core/> (visited June 19, 2018).

¹⁰⁶ See TIA Comments at 73 (mentioning SpiderCloud, Tarana, Phazor, Mimoso, Ceragon, Radwin, Siklu, and Aviat).

CommScope, and Corning.¹⁰⁷ Importantly, these solutions can be cost-effective alternatives to macrocell deployments for rural service providers.¹⁰⁸ For example, Airspan Networks offers an LTE-Advanced solution specifically tailored to address the rural challenge, observing that creating smaller coverage areas can remove complexity and costs, and that smaller coverage areas allow spectrum re-use which provides effective throughput and order of magnitude better than typical macrocell deployments.¹⁰⁹ Although there are approximately 300,000 cell sites in use in the United States, the use of small cells is growing rapidly with between 100,000 and 150,000 being potentially installed nationwide by the end of 2018.¹¹⁰

End-to-end design and customer service. Many vendors provide end-to-end design solutions and customer service for carrier customers – not merely “discrete components” as CCA claims.¹¹¹ For example, Calix offers a large suite of services to service provider customers, and even provides customers with dedicated advice about how to obtain funding from the

¹⁰⁷ Cisco, *Universal Small Cell 7000 Series*, <https://www.cisco.com/c/en/us/products/wireless/universal-small-cell-7000-series/index.html> (visited June 20, 2018); CommScope, *C-RAN Small Cells*, <https://www.commscope.com/Product-Catalog/Networking-Systems/Product/Small-Cells/C-RAN-Small-Cells/> (visited June 20, 2018); Corning, *Distributed Antenna System (DAS)*, <https://www.corning.com/worldwide/en/products/communication-networks/applications/wireless-networks/wireless-das.html> (visited June 20, 2018); Corinne Reichert, *Fujitsu unveils small cell mmWave 5G tech*, ZDNET, Oct. 11, 2017, <https://www.zdnet.com/article/fujitsu-unveils-small-cell-mmwave-5g-tech/>.

¹⁰⁸ See Small Cell Forum, *Rural small cell market size, business case, challenges & solutions*, Dec. 2013, http://scf.io/en/documents/047_Extending_rural_and_remote_coverage_using_small_cells.php.

¹⁰⁹ Airspan Networks, *Rural Solutions*, <http://www.airspan.com/rural-solutions-1/> (visited June 20, 2018).

¹¹⁰ *Twentieth Mobile Competition Report*, 32 FCC Rcd at 8998 ¶ 43.

¹¹¹ See CCA Comments at 37 & n.80.

Commission’s forthcoming CAF Phase II universal service auction.¹¹² Ericsson offers a full range of services from network design and optimization through rollout and various support service packages.¹¹³ Nokia offers services in network planning and implementation, along with systems integration of equipment in multivendor network architectures.¹¹⁴ Samsung offers solutions from professional service and network deployment to maintenance.¹¹⁵

Third-party suppliers. Besides the original equipment manufacturers themselves, there is a significant network of third-party suppliers that deliver end-to-end solutions for their carrier customers. For example, VERTICOM partners with carriers to design, acquire, develop, and maintain networks, and prominently advertises that it is a “solution architect[] with the turnkey in-house capabilities to build and maintain what [it] engineer[s].”¹¹⁶ Communications logistics company KGPCo offers “turnkey” solutions “from design and deployment to equipment and field services,” holding itself out as a “convenient and cost-effective one-stop alternative to

¹¹² Calix, *Services*, <https://www.calix.com/services.html> (visited June 19, 2018); Calix, *Calix CAF Phase II Auction Resources*, <https://www.calix.com/pages/caf2-auction-resources.html> (visited June 19, 2018).

¹¹³ Ericsson, *Ericsson Network Services*, <https://www.ericsson.com/ourportfolio/network-services> (visited June 19, 2018).

¹¹⁴ Nokia, *Services*, <https://networks.nokia.com/services> (visited June 19, 2018); Nokia, *Systems Integration*, <https://networks.nokia.com/services/systems-integration> (visited June 19, 2018).

¹¹⁵ Samsung, *Samsung Global Services*, <https://www.samsung.com/global/business/networks/services/> (visited June 19, 2018).

¹¹⁶ VERTICOM, *About Us*, <https://verticom.net/> (visited June 19, 2018).

[original equipment manufacturers].”¹¹⁷ Tescoco provides solution architecture including system design and solution development, including experience with Tier 1 and regional carriers.¹¹⁸

Downtime. Some carriers have assumed there would be significant network downtime associated with any replacement of their Huawei or ZTE equipment, and they therefore include costs such as lost roaming revenue in their overall cost estimates for replacement.¹¹⁹ However, this fails to account for the fact that other manufacturers and suppliers can and would take proactive steps to greatly reduce or even eliminate any downtime associated with a transition. For example, Ericsson specifically markets its radio access network (“RAN”) modernization and swap services to carriers for radios, baseband units, and/or controllers, with the specific objectives of minimum impact on a carrier’s end-users during network changes, and high-quality and fast modernizations and swaps.¹²⁰ Likewise, Nokia notes that the benefits of its network modernization projects include “timely delivery,” “high network and service quality,” and “no interruptions to customer experience during on-going projects.”¹²¹

¹¹⁷ KGPCo, *Whatever You Envision, We Can Implement*, <http://www.kgplogistics.com/das-small-cell.html> (visited June 19, 2018).

¹¹⁸ Tescoco, *Solution Architecture*, <https://www.tescoco.com/services/enhanced-services?tab=2> (visited July 2, 2018).

¹¹⁹ CCA Comments at 31; *see, e.g., id.* at DiRico Decl. ¶ 4 (“During installation of the new equipment, Viaero will have to forego as much as \$50 million in roaming fees from several national carriers.”); *id.* at Woody Decl. ¶ 4 (“The downtime from installing new equipment would cause Union to forego another \$26 million in roaming fees annually from a larger carrier.”).

¹²⁰ Ericsson, *RAN Modernization and Swap*, <https://www.ericsson.com/ourportfolio/network-services/ran-modernization-and-swap> (visited June 19, 2018).

¹²¹ Nokia, *Network Modernization*, <https://networks.nokia.com/services/network-modernization> (visited June 25, 2018).

Security through network diversity. NTCA suggests that the Commission’s proposed action “is in direct opposition to other various cybersecurity best practices,” specifically that “network diversity, particularly regarding equipment, is a security best practice, while this proposal, if enacted, would result in more homogenous networks.”¹²² As explained above, the marketplace for equipment of all kinds – from core to access – is robustly competitive, rendering NTCA’s concerns moot.

2. Other Companies Provide Reasonably Comparable Alternatives for All Huawei Products Specifically Identified by Huawei.

Huawei claims that it “brought advanced technology and much needed competition to the U.S.,” noting that its 4T4R Single Radio Area Network (“RAN”) products helped its customers improve service area coverage.¹²³ In a declaration attached to Huawei’s comments, one of its senior vice presidents goes further:

In 2013, Huawei was the first to deploy the 700 MHz LTE coverage extension feature. Just last year, Huawei was the first vendor to launch 8T8R TD-LTE products to support 3.5 GHz CBRS. It is my understanding that currently no other equipment vendors in the U.S. are willing and/or able to bring these innovative and industry leading solutions to the U.S. market.¹²⁴

Collectively, these assertions are either misleading or simply incorrect. Whether 3.5 GHz CBRS equipment has been “brought ... to the U.S. market” is irrelevant because the Commission is currently reviewing the rules for that band and commercial operations have not yet started.¹²⁵ In any event, other vendors are actively moving ahead in this area. For example, Verizon recently

¹²² NTCA Comments at 21.

¹²³ Huawei Comments at 10 (citing Ex. C, Dowding Decl. ¶ 29).

¹²⁴ *Id.*, Ex. C, Dowding Decl. ¶¶ 29-30.

¹²⁵ *See generally Promoting Investment in the 3550-3700 MHz Band*, Notice of Proposed Rulemaking and Order Terminating Petitions, 32 FCC Rcd 8071 (2017).

announced that it is collaborating with Corning, Ericsson, Federated Wireless, Google, Nokia, and Qualcomm to test 3.5 GHz CBRS end-to-end solutions.¹²⁶ Meanwhile, other companies are providing 8T8R antenna solutions as well.¹²⁷ Regardless, U.S. carriers large and small have a wide variety of options to meet their equipment needs; there is no product offering from Huawei for which a reasonable market alternative does not exist.

Next, Huawei points out that U.S. telecommunications service providers seek to use software-defined networking (“SDN”) and network functions virtualization (“NFV”) in order to “reduce CAPEX and OPEX, improve efficiency, introduce more diverse services, and to compete more effectively with OTTs....”¹²⁸ This is true, but numerous TIA members provide SDN and NFV solutions, contrary to Huawei’s further claim that “it is difficult for [such service providers] to find vendors in the U.S. to willingly participate, implement and build out their vision.”¹²⁹ For example, Ericsson recently announced that four regional service providers – Carolina West Wireless, Cellcom, Chariton Valley, and East Kentucky Networks – are now able

¹²⁶ Press Release, Verizon, *Verizon Takes Industry Lead in Working with Key Partners to Drive Advancements on CBRS Spectrum*, Apr. 5, 2018, <https://www.verizon.com/about/news/verizon-takes-industry-lead-working-key-partners-drive-advancements-cbrs-spectrum>.

¹²⁷ See, e.g., CommScope, *Product NewsFLASH: 8T8R Beamforming Base Station Antenna Family: New Product*, Dec. 15, 2017, https://www.commscope.com/Docs/ProductNewsFLASH/PB-112413-EN_8T8R_Beamforming_BSA.pdf.

¹²⁸ Huawei Comments, Ex. C, Dowding Decl. ¶ 31; see generally Ed Tittel, *SDN vs. NFV: What’s the difference?*, Cisco, <https://www.cisco.com/c/en/us/solutions/software-defined-networking/sdn-vs-nfv.html> (visited June 25, 2018).

¹²⁹ Huawei Comments, Ex. C, Dowding Decl. ¶ 31.

to offload end-to-end management of monitoring, troubleshooting, configuration, and optimization of their networks.¹³⁰ In the words of CCA's President and CEO, Steven Berry:

Many rural and regional operators in the United States are challenged with offering their customers robust wireless services while operating efficient and profitable networks. Ericsson, a long-time CCA member, continues to demonstrate a deep understanding of the regional operator space, and solutions like this one will help carriers to stay competitive with larger operators.¹³¹

Other vendors maintaining portfolios of SDN / NFV offerings for carrier customers include ADTRAN, Cisco, Infinera, Nokia, and Samsung, among others.¹³²

D. The Commission Should Consider Remedial Steps for Affected USF Recipients While Taking Caution to Ensure Such Measures Do Not Undermine the Purpose of the Rule.

Affected USF recipients cannot reasonably assert a reliance interest in the Commission's previous policies because the Commission explicitly states that any adopted rule will not be applied retroactively.¹³³ However, TIA appreciates that some USF recipients may require a glide path to transition away from equipment that, it has now been shown, presents certain national

¹³⁰ Ericsson, *US Operators Embrace Ericsson Network Management as a Service*, Mar. 26, 2018, <https://www.ericsson.com/en/news/2018/3/enm-as-a-service---usa> (visited June 25, 2018).

¹³¹ *Id.*; see also Ericsson, *Network Functions Virtualization*, <https://www.ericsson.com/digital-services/trending/network-functions-virtualization> (visited June 25, 2018); Ericsson, *Ericsson Cloud SDN*, <https://www.ericsson.com/ourportfolio/digital-services-products/cloud-sdn> (visited June 25, 2018).

¹³² See, e.g., ADTRAN, *Defining the Future Network*, <https://www.adtran.com/index.php/broadband-access/sdn-nfv> (visited June 25, 2018); Cisco, *SDN for Service Providers*, <https://www.cisco.com/c/en/us/solutions/service-provider/software-defined-networks-sdn-service-providers/index.html> (visited June 25, 2018); Infinera, *Transport SDN*, <https://www.infinera.com/technology/transport-sdn/> (visited June 25, 2018); Nokia, *SDN & NFV*, <https://networks.nokia.com/portfolio/sdn-nfv> (visited June 25, 2018); Samsung, *Cloud & NFV (AdaptiV)*, <https://www.samsung.com/global/business/networks/solutions/cloud-nfv/> (visited June 25, 2018).

¹³³ Notice ¶ 17; see CCA Comments at 32-34 (arguing that carriers have substantial reliance interests), 40-42 (related to its due process argument).

security risks. TIA is sympathetic to the claim that “[p]roviders should not be punished retroactively for using equipment that they previously selected in a reasonable and prudent manner.”¹³⁴ Therefore, as necessary, TIA encourages the Commission to consider reasonable means to mitigate the burdens incurred by recipients that may be affected.

Compliance costs could be mitigated through a more narrowly tailored rule and an appropriate transition plan with a robust and meaningful waiver process. That said, we urge caution when considering “grandfather clauses” that would undermine the purpose of the rule itself – to protect USF networks from suppliers that pose a national security threat. Furthermore, given the serious nature of the threat posed, the average useful life of such equipment, the fact that entities have been on notice that the federal government has serious concerns with such suppliers, and because many entities have been or were able to choose not to use suppliers named in the notice due to acknowledged security concerns, provisions providing, for example, a 10-year implementation timeframe or grandfathering existing contracts for future upgrades or services seem unreasonable and would undermine the efficacy of the rule itself.

Given the importance of maintaining robust service among these communities and the economic challenges that USF recipients face, we agree with CCA that the Commission should consider adopting reasonable measures to accommodate affected recipients’ transition as necessary.¹³⁵ However, as the Commission considers appropriate steps to aid USF recipients in implementing this rule, mitigation measures should not undermine the rule’s legitimacy or effectiveness.

¹³⁴ WTA Comments at 6.

¹³⁵ See CCA Comments at 44-46.

Finally, while the Commission should consider the potential impact on supported companies of any proposed actions, the Commission's universal service policies are of course designed to ensure the availability of service to all consumers, businesses and community anchor institutions, not to ensure the success of any one company. To that end, with respect to claims that consumers will lose access to service if costs are increased for select companies, while there may be some areas in which the companies identified by CCA are the only provider serving an area, TIA notes that the coverage areas of these companies all appear to be significantly overlapped by multiple wireless competitors.¹³⁶ Thus, the claimed elimination of service to *consumers* may be significantly overstated by CCA.

¹³⁶ Compare FCC, *3G or Better Coverage by Number of Providers-YE 2016* (updated Sept. 27, 2017), <https://www.fcc.gov/reports-research/maps/3gorbetter-number-providers-ye-2016> and FCC, *Residential Fixed Internet Access Service Providers by Census Block* (updated Apr. 3, 2018), <https://www.fcc.gov/reports-research/maps/residential-fixed-internet-access-service-providers-by-census-block-dec-2016> with SI Wireless LLC d/b/a MobileNation Coverage Map, <https://www.mymobilenation.com/coverage> (visited June 28, 2018); NE Colorado Cellular d/b/a Viaero Wireless Coverage Map, <http://www.viaero.com/support/help-center/national-coverage-map/local-coverage> (visited June 28, 2018); James Valley Telecommunications Coverage Map, <http://www.jamesvalley.com/residential/cell-phone/cell-phone-coverage> (visited June 28, 2018); United Telephone Association, Inc. Coverage Map, <https://decisiondata.org/coverage/united-telephone-association-availability> (visited June 28, 2018); Nemont Telephone Cooperative, Inc. Coverage Map, <https://www.nemont.com/services/wireless/coverage-map> (including Sagebrush Cellular's service area) (visited June 28, 2018); Union Telephone Company d/b/a Union Wireless Coverage Map, <https://www.unionwireless.com/wireless-coverage> (visited June 28, 2018); Pine Belt Cellular Communications Coverage Map, <https://decisiondata.org/coverage/pine-belt-cellular-availability> (visited June 28, 2018); Mark Twain Communications Company Coverage Map, <https://decisiondata.org/coverage/mark-twain-communications-company-availability> (visited June 28, 2018); Claro Puerto Rico Coverage Map, <https://opensignal.com/networks/puerto-rico/claro-coverage> (visited June 28, 2018).

IV. COMPANIES SPECIFIED IN THE NOTICE MAY BE REASONABLY DISTINGUISHED FROM OTHERS DUE TO NATIONAL SECURITY CONCERNS.

The record in this proceeding, including TIA’s comments describing actions moving on parallel tracks, provides detailed discussion of the specific concerns that the U.S. government and closely allied nations have about the potential for cyberespionage and sabotage arising from suppliers closely connected to the Chinese state.¹³⁷ These concerns are both longstanding and specific. Nevertheless, Huawei suggests that the Commission “fails to explain its singular focus on ‘Chinese telecommunications companies’ – raising an inference that it is discriminating invidiously rather than genuinely promoting national security.”¹³⁸ Far from invidious discrimination, the Commission’s citation in the Notice of certain companies from China and Russia is a logical starting point in an effort to identify companies whose equipment or services may pose “a national security threat to the integrity of communications networks or the communications supply chain.”¹³⁹

Huawei has argued that there is no legitimate basis for action against it, nor that there is any reason to distinguish between it and other companies with facilities in or connections to China. While TIA does not have access to classified intelligence that may underlie specific U.S. government concerns, there are multiple characteristics directly pertinent to Commission’s security concerns by which Huawei and ZTE can be distinguished from other suppliers of similar

¹³⁷ See TIA Comments at 10-18 (describing security concerns and actions). In response to Huawei’s comments, this section focuses on the concerns specific to Huawei and ZTE. TIA recognizes that the Notice also cited Kaspersky Lab as a company of concern, and TIA’s opening comments stand with regard to concerns about that company. See *id.* at 12-13, 16, 17.

¹³⁸ Huawei Comments at 45.

¹³⁹ See Notice, App. A.

equipment and services. To begin with, consider the backdrop of China’s increasingly aggressive military posture vis-à-vis the United States and history of state-sponsored cyberespionage,¹⁴⁰ along with a legal environment that appears to offer very substantial latitude to Chinese intelligence authorities. In addition, there are myriad company-specific factors that give cause for concern, particularly when considered in their entirety. These include (1) the role of the Chinese Communist Party (“CCP”) at Huawei and ZTE, (2) their acceptance of billions of dollars in state-backed funding to aid their international expansion, (3) the companies’ involvement in strategic state industrial development plans, and (4) their position as potential conduits to channel advanced commercial technologies into China’s military. Finally, ZTE’s admitted evasion of U.S. national security laws¹⁴¹ and failure to abide by subsequent commitments to American authorities offers further proof that the Commission’s scrutiny is well justified.

TIA, along with virtually every other commenter, believes that the Commission should not make independent determinations regarding the security threat posed by particular companies.¹⁴² As we have argued, such determinations should derive from broader processes

¹⁴⁰ See, e.g., James R. Clapper, Director of National Intelligence, Worldwide Threat Assessment of the U.S. Intelligence Community, Statement for the Record before the U.S. Senate Armed Services Committee, Apr. 18, 2013, at 8-9, (“Clapper Statement”), https://www.dni.gov/files/documents/Intelligence%20Reports/UNCLASS_2013%20ATA%20SFR%20FINAL%20for%20SASC%2018%20Apr%202013.pdf.

¹⁴¹ U.S. Department of Commerce, Bureau of Industry and Security, *Order Activating Suspended Denial Order Relating to Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd.*, Apr. 15, 2018, https://www.commerce.gov/sites/commerce.gov/files/zte_denial_order.pdf.

¹⁴² TIA Comments at 27, 54, 58-60; see also, e.g., CTIA Comments at 13, 16-18; EchoStar/Hughes Comments at 7-8; ITTA Comments at 1-4; USTelecom Comments at 9-10; CCA Comments at 5; PRTC Comments at 5.

that include Congress, the President, or agencies with appropriate expertise. Nevertheless, given that Huawei is arguing that there is no legitimate basis for FCC action against it, we summarize below the overwhelming evidence in the record that supports such action.

A. The Record Regarding Specific Suppliers Named in the Notice Is Compelling.

The record in this proceeding now constitutes an overwhelming catalog of the concerns that the U.S. government has about the potential for cyberespionage and sabotage arising from Huawei's and ZTE's close ties to the Chinese state. Beginning with the materials and actions cited in the Notice itself,¹⁴³ the record should now include not just the initial comments but the broader Congressional and public policy discourse and law enforcement activities that have taken place in parallel to this proceeding,

First, the initial comments provide a litany of U.S. and allied government concerns and actions related to these companies, both in the years before the Commission adopted the Notice and in the subsequent weeks before comments were submitted on June 1, 2018. As detailed in TIA's and other stakeholders' comments in this proceeding, U.S. government concerns about Huawei and ZTE are longstanding and have led to several significant concrete actions, including statutory restrictions on procurement by federal agencies, administrative restrictions, discouragement of commercial use, and prohibitions of corporate acquisition transactions.¹⁴⁴

Similar concerns among governments and influential stakeholders in the United States' closest

¹⁴³ Notice ¶¶ 4-6; *see also* HPSCI Report; Letter from Senator Tom Cotton *et al.* to FCC Chairman Ajit Pai, Dec. 20, 2017; National Defense Authorization Act for Fiscal Year 2018 § 1656, Pub. L. 115-91, 131 Stat. 1283, 1762 (“FY18 NDAA”).

¹⁴⁴ TIA Comments at 11-12; *see also* USTelecom Comments at 5-8.

national security and intelligence allies – including Australia, Canada, the United Kingdom, and South Korea – have led them to also consider or implement related actions.¹⁴⁵

These national security concerns and related actions constitute a refutation of the notion that the record “do[es] not identify any specific threat from Huawei” or that nothing “establishes any basis for labeling Huawei as a threat to national security.”¹⁴⁶ Instead, the record demonstrates that these companies are not suppliers worthy of trust, much less public funding. Apart from Huawei’s own comments and some conclusory assertions from CCA,¹⁴⁷ all other commenters in this proceeding either (1) cite and support these U.S. and allied government concerns, or (2) do not address them at all. Only Huawei has seriously attempted to rebut any of the national security concerns raised by U.S. and allied governments.

Second, even in the weeks since the Commission received opening comments in this proceeding, the Senate has overwhelmingly passed legislation that would take further action against Huawei and ZTE specifically. The FY19 National Defense Authorization Act (“NDAA”), passed on June 18 by the bipartisan vote of 85-10, would bar U.S. government procurement from contractors that use Huawei and ZTE equipment and services.¹⁴⁸ The

¹⁴⁵ TIA Comments at 13-14; *see also* Rod McGuirk, *Huawei Executive Warns Australia Risks Economy with 5G Ban*, WASH. POST, June 27, 2018, https://www.washingtonpost.com/world/asia_pacific/huawei-executive-warns-australia-risks-economy-with-5g-ban/2018/06/27/1a52ab2e-79ce-11e8-ac4e-421ef7165923_story.html (“Australia barred Huawei, the world’s largest telecommunications equipment supplier, on national security grounds from bidding for contracts in 2011 for the national broadband network which is being rolled out countrywide. According to media reports, the government is now poised to ban Huawei from supplying 5G networks, the next evolution in phone technology that will start commercial services in Australia next year.”).

¹⁴⁶ Huawei Comments at 89-90.

¹⁴⁷ *Id.* at 89-91; CCA Comments at 37-40.

¹⁴⁸ John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 6702, H.R. 5515, 115th Cong. (printed as passed the Senate, June 19, 2018) (“Senate FY19 NDAA”).

provision is very similar to a provision passed by the House of Representatives on May 24 in its version of the bill,¹⁴⁹ and thus will likely be easily reconciled and adopted in the final version of the bill in the near future. Additionally, the Senate NDAA contained an extraordinary provision that would overturn the President’s negotiated deal regarding ZTE’s export control violations.¹⁵⁰

Thus, CCA’s claim that the “entirety” of the evidence against Huawei is the October 2012 HPSCI report¹⁵¹ is simply false, and it grossly understates the national security concerns that the U.S. government and others have raised regarding Huawei and ZTE. The 2012 report was merely one step – not the last – in the government’s broader concerns and (ongoing) investigations of Huawei and ZTE, and it started a prolonged and measured set of inquiries in Congress and the Executive Branch on which the Commission may properly rely. During the course of this very proceeding, ZTE has been the subject of highly-publicized Presidential-level negotiations due to its previous egregious violations of U.S. export controls laws and subsequent false statements regarding its implementation of the settlement agreement regarding those violations.¹⁵² Setting aside the government’s specific concerns about cyberespionage and

¹⁴⁹ National Defense Authorization Act for Fiscal Year 2019 § 880, H.R. 5515, 115th Cong. (Engrossed in House, May 24, 2018).

¹⁵⁰ Senate FY19 NDAA § 6702(a).

¹⁵¹ CCA Comments at 37.

¹⁵² See TIA Comments at 79 (describing history through June 1); see, e.g., Erica Werner, *White House Aims to Kill Senate Attempt to Reimpose Penalties on ZTE*, WASH. POST, June 13, 2018, <https://www.washingtonpost.com/news/business/wp/2018/06/13/white-house-pushes-back-on-congressional-attempt-to-block-zte-deal/> (discussing White House efforts to block legislation that would reimpose penalties on ZTE); Patricia Zengerle, *U.S. Senators Want Trump to Reconsider Lifting Ban on China’s ZTE*, REUTERS, June 26, 2018, <https://www.reuters.com/article/us-usa-china-zte-senate/u-s-senators-want-trump-to-reconsider-lifting-ban-on-chinas-zte-idUSKBN1JM304> (discussing a recent letter from senators to the President requesting that he reconsider his agreement with ZTE that lifted April’s DOC sanctions).

sabotage capabilities, ZTE's admitted violations of laws that protect U.S. national security manifestly and incontrovertibly contradict any claim the company may have previously had to being a supplier that the U.S. government can trust on national security issues. For its part, Huawei is reportedly under investigation for export controls violations that are similar to – and perhaps the model for – those of ZTE.¹⁵³

Finally, as noted above, perhaps the most telling element of the record is that apart from Huawei's claims regarding its own conduct and a few observations from CCA, the record contains no meaningful defense of these companies and therefore leaves the concerns described in the Notice, as supplemented by TIA's comments and others, entirely un rebutted. Meanwhile, ZTE did not even file initial comments in this proceeding.

B. Significant Strategic Risks Have Been Identified Regarding the Chinese Government and Closely Connected ICT Companies.

There is nothing arbitrary or discriminatory about the FCC's concern regarding the potential threat posed by certain Chinese suppliers. As a starting point, the U.S. government has had a longstanding willingness to identify China's espionage capabilities and related technological ambitions as a potential threat.¹⁵⁴ In recent years the national security, defense and trade arms of the U.S. government have all taken increasingly public stances in identifying risks associated with China. These include the Chinese government's more assertive military posture, its aggressive efforts to acquire and develop technologies with military uses, and its

¹⁵³ See TIA Comments at 79 (citing Paul Mozur, *Huawei, Chinese Technology Giant Is Focus of Widening U.S. Investigation*, N.Y. TIMES, Apr. 26, 2017, <https://www.nytimes.com/2017/04/26/business/huawei-investigation-sanctions-subpoena.html>) (describing a U.S. government investigation that found that ZTE had conspired to sell telecommunications equipment to Iran and North Korea, in violation of U.S. export sanctions, and implicated another as-yet-unnamed equipment supplier engaged in similar activity, and that some believe this company could be Huawei).

¹⁵⁴ See, e.g., Clapper Statement at 8-9.

economically harmful trade practices. Other concerns include the country's legal system, including its recently-adopted Cybersecurity Law, and the existing and increasing pressures that nominally-private enterprises face under the Chinese system.

Strategic concerns. In 2017, the President's National Security Strategy recognized China as a strategic competitor with interests adversarial to the United States. The Strategy concluded that both China and Russia are seeking "to challenge American power, influence, and interests, attempting to erode American security and prosperity."¹⁵⁵ Both countries are "developing advanced weapons and capabilities that could threaten our critical infrastructure and our command and control architecture,"¹⁵⁶ the report said. Moreover, "China gathers and exploits data on an unrivaled scale and spreads features of its authoritarian system, including corruption and the use of surveillance. It is building the most capable and well-funded military in the world, after our own. Its nuclear arsenal is growing and diversifying."¹⁵⁷ Similar concerns specific to China and its aggressive attempts to acquire U.S.-developed technology were identified in a 2018 report commissioned by DOD, which concluded that the United States lacks a strategy to respond to China's efforts to extract American technology that can be redirected for military uses.¹⁵⁸

¹⁵⁵ President Donald J. Trump, *National Security Strategy of the United States of America*, at 52 (Dec. 2017), <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

¹⁵⁶ *Id.* at 8.

¹⁵⁷ *Id.* at 25.

¹⁵⁸ Michael Brown & Pavneet Singh, Defense Innovation Unit Experimental (DIUx), *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation*, Jan. 2018, at 3, [https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_\(1\).pdf](https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf) (visited June 28, 2018).

U.S. trade officials have also publicly described Chinese policies regarding technology acquisition as a threat to global commercial norms. In May 2018, U.S. Ambassador to the WTO Dennis Shea summed up American complaints in a statement to the WTO General Council, explaining as follows:

China ... is consistently acting in ways that undermine the global system of open and fair trade. [This includes] market access barriers too numerous to mention; forced technology transfers; intellectual property theft on an unprecedented scale; indigenous innovation policies and the Made in China 2025 program; discriminatory use of technical standards; massive government subsidies that have led to chronic overcapacity in key industrial sectors; and a highly restrictive foreign investment regime.¹⁵⁹

As Shea noted, China is a well-known perpetrator of IP theft, and state-backed cyberespionage continues to offer a valuable channel to obtain U.S. technology and to aid the favored, state-supported companies known as “national champions.” The U.S. Section 301 proceeding undertaken by the United States Trade Representative (“USTR”) to investigate and document unfair Chinese trade practices determined that:

State-sponsored cyber intrusions originating from China into U.S. commercial networks occur alongside China’s institutional framework for promoting its industrial and technological development through a state-led model in which state-owned enterprises and national champions are the recipients of extensive state support. In sum, the evidence indicates that China continues its policy and practice, spanning more than a decade, of conducting and supporting cyber-enabled theft and intrusions into the commercial networks of U.S. companies.¹⁶⁰

¹⁵⁹ Ambassador Dennis Shea, Deputy U.S. Trade Representative and U.S. Permanent Representative to the WTO, Statement as delivered to the WTO General Council, Geneva, May 8, 2018, <https://geneva.usmission.gov/2018/05/16/ambassador-dennis-sheas-statement-at-the-wto-general-council/>.

¹⁶⁰ Office of the U.S. Trade Representative, *Findings of the Investigation into China’s Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, at 171 (Mar. 22, 2018), <https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF>.

The CCP and China's legal framework for ICT companies. Huawei has submitted a declaration from two Chinese lawyers, Jihong Chen and Jianwei Fang, asserting that “the Chinese government is not authorized to compel telecommunication equipment manufacturers to hack into products they make to spy on or disable communications....”¹⁶¹ This is misleading. Even stipulating that legal authority is indeed relevant to China’s espionage and sabotage operations, the relevant authority is not China’s government, but rather the CCP. As discussed further below, in China’s legal framework, the Constitution enshrines the Party as the ultimate authority.¹⁶² The CCP – not the government – directs matters of state, and there are no constitutional checks on the Party’s power. Thus, Party officials have considerable leeway to influence interpretations of the law – for instance, regarding cyberespionage or sabotage.

Chen and Fang themselves cite provisions of China’s National Intelligence Law that provide grounds for the state to take actions deemed necessary for intelligence work, including not only a stipulation that organizations and citizens should support state intelligence work¹⁶³ but a related provision that intelligence agencies may demand such assistance.¹⁶⁴ They conclude that

¹⁶¹ Huawei Comments, Ex. E, Chen & Fang Decl. ¶ 8.

¹⁶² See *infra* sec. IV-C & n.181.

¹⁶³ PRC National Intelligence Law, art. 7, adopted June 27, 2017, http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529.htm (第七条 任何组织和公民都应当依法支持、协助和配合国家情报工作，保守所知悉的国家情报工作秘密。国家对支持、协助和配合国家情报工作的个人和组织给予保护 “All organizations and citizens shall, in accordance with relevant laws, support, assist, and cooperate with national intelligence work, and keep confidential the secrets of the state intelligence work known to them. The State shall protect individuals and organizations that support, assist and cooperate with national intelligence work.”).

¹⁶⁴ *Id.* art. 14 (第十四条 国家情报工作机构依法开展情报工作，可以要求有关机关、组织和公民提供必要的支持、协助和配合。 “National intelligence agencies conducting intelligence work in accordance with the law are permitted to require relevant agencies, organizations and citizens to provide necessary support, assistance and cooperation.”).

the National Intelligence Law could not be used to compel companies to plant backdoors and spyware because doing so would “infringe the manufacturer’s legitimate rights and interests.” However, it would seem fair to assume that in calculations made by Chinese intelligence agencies, concerns of state security would trump those of manufacturing interests.

Moreover, the Party is highly sensitive to perceived threats to its authority. For this reason, it may identify and seek to act upon so-called “threats” to national security that would not be perceived as such in the United States. Consider China’s Counter-Terrorism Law, which Chen and Fang cite in their declaration. Oddly enough, they seem to offer up the law as an example of the legal boundaries of state power.¹⁶⁵ But if the intention is to show that Beijing fears overstepping its authority, the Counter-Terrorism Law is a particularly unconvincing choice of statute. The law contains a sweeping definition of terrorism that includes “disruptions to public order.”¹⁶⁶ It does not define what a “threat to public order” actually means, apparently reserving the right for the state to make that determination. Thus, Chen and Fang are attempting to claim limits for a law whose explicit wording allows for the maximum exercise of state power.

Not surprisingly, the security laws to which they refer do not expressly compel telecommunications companies to hack into their own products in order to spy or disrupt communications. The laws employ language that is far more politic – and vague – thus allowing the state vast discretionary authority. For example, Article 28 in China’s Cybersecurity Law (cited by Chen and Fang) says that in the interests of national security, network operators must

¹⁶⁵ Huawei Comments, Ex. E, Chen & Fang Decl. ¶ 8.

¹⁶⁶ Counter-Terrorism Law of the People’s Republic of China, art. 3, adopted Dec. 27, 2015, http://www.npc.gov.cn/npc/xinwen/2015-12/28/content_1957401.htm (defining “terrorist activities” to include “disruptions to public order”).

provide “technical support and assistance” upon request.¹⁶⁷ The law offers no limitation on what form such help may take, but it would be dangerously naïve to believe that the China might possibly construe “technical support and assistance” so narrowly as to preclude requests for cyber espionage or sabotage operations where Huawei or ZTE have operational capability.

Perhaps mindful of the problems above, Chen and Fang next seek to argue that the Cybersecurity Law does not apply to Huawei anyway, on the theory that the company is not a “network operator.”¹⁶⁸ However, the meaning of this term is still in question. The Cybersecurity Law defines “network operator” to mean the “owner and administrator of the network, and network service operator.”¹⁶⁹ In practice, Chinese authorities have yet to clearly articulate to whom the definition applies. The foreign business community has proceeded on the assumption that it refers to companies *in general* and as a result, has devoted much time and resources to trying to understand how to comply with its loosely-worded obligations.¹⁷⁰ If major American ICT companies in China feel compelled to comply with a major new law on cybersecurity, it stands to reason that Huawei, as one of China’s leading technology firms, would be subject to it as well.

¹⁶⁷ Cybersecurity Law of the People’s Republic of China, art. 28, adopted Nov. 7, 2016 (“The network operators shall provide technical support and assistance when the public security organs or national security organs conduct activities aimed to safeguard national security and investigate crimes according to law.”) (“China Cybersecurity Law”); Huawei Comments, Ex. E, Chen & Fang Decl. ¶ 9.

¹⁶⁸ Huawei Comments, Ex. E, Chen & Fang Decl. ¶ 9.

¹⁶⁹ China Cybersecurity Law art. 76 (3).

¹⁷⁰ Liza Lin & Yoko Kubota, *U.S. Tech Firms Spooked By China’s Arcane Cybersecurity Law*, WALL ST. J., Dec. 6, 2017, <https://www.wsj.com/articles/chinas-blurry-cyber-laws-give-u-s-tech-companies-no-security-1512558004>.

Far from circumscribing China’s government’s power over companies like Huawei and ZTE, the Cybersecurity Law, the Counter-Terrorism Law, and other national security legislation create substantial room for state intervention and influence. In the current political environment, China’s security laws would be leveraged to justify state intervention, rather than to limit state authority. It is impossible to know what form such intervention may take, but China’s extensive history of state-backed cyberespionage¹⁷¹ suggests it sees few limits on its authority to exploit digital infrastructure for state gains.

Pressure on private companies. Huawei appears to suggest in its comments that because it is nominally private under Chinese law, it therefore functions as an independent and autonomous actor in a free market – akin to what one might expect of a privately held or publicly-traded U.S. company.¹⁷² This is an unconvincing argument given the close connections between the Party, state and private enterprise in China. As one legal academic explains:

[J]ust because the state is not the dominant shareholder [in China] does not mean that the state does not have a role. Instead, as some commentators have noted, the labels associated with formal shareholding structures can mislead, because “the boundary between state and private ownership of enterprise is often blurred in contemporary China.”¹⁷³

¹⁷¹ Mandiant, *APT1: Exposing One of China’s Cyber Espionage Units*, at 3-4 (2013), <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>.

¹⁷² Huawei Comments at 87-88 (“private enterprises are *legally* independent of the Chinese government”) (emphasis added); *id.*, Ex. D, Ye Decl. ¶ 9 (“Chinese private enterprises are *legally* independent from the PRC government and they are able to make commercial decisions independently.”) (emphasis added); *id.* ¶ 13 (“there is no *legal* basis for the PRC government to interfere in the decision-making of any privately owned enterprises or companies including Huawei”) (emphasis added); *id.* ¶ 15 (“I am not aware of any evidence suggesting that Huawei, being a private company owned by its employees, has been *unlawfully* interfered with, directly or indirectly.”) (emphasis added).

¹⁷³ Mark Wu, *The ‘China, Inc.’ Challenge to Global Trade Governance*, 57 HARVARD INT’L LAW J. 283, Spring 2016.

The same observer rhetorically queries, “How have the Party and the state forged links with private firms?” and responds:

“Numerous mechanisms abound. State-owned banks, for example, finance private firms. The state enlists industry associations and local chambers of commerce to coordinate action within a given sector and/or region and to assist with trade disputes. The state also establishes informal, backdoor channels with private firms to communicate about regulatory issues. At times, the state, or an investment fund with close links to the Party-state, will go so far as to purchase equity in private firms. Finally... Party committees exist inside most private firms.¹⁷⁴

The CCP has become more assertive in the private sector since President Xi took office, with a growing expectation that private enterprise be attuned to and accommodate Xi’s Party directives.¹⁷⁵ “Party members are expected to spend more time studying Xi Jinping Thought, the president’s political theory, in office hours or in time-consuming off-site retreats,” and “business executives...are worried about a trend toward growing party interference.”¹⁷⁶ In mid-June, China’s securities regulator called for listed companies to devote more attention to internal Party-building efforts.¹⁷⁷ The Party has also broadened its focus from state-owned firms to

¹⁷⁴ *Id.*

¹⁷⁵ See, e.g., Chun Han Wong & Eva Dou, *Foreign Companies in China Get a New Partner: The Communist Party*, WALL ST. J., Oct. 29, 2017, <https://www.wsj.com/articles/foreign-companies-in-china-get-a-new-partner-the-communist-party-1509297523> (noting that Xi told a group of business leaders to guide staff to honor the “glorious tradition of listening to the party’s words and following the party’s path”).

¹⁷⁶ Simon Denyer, *Command and Control: China’s Communist Party Extends Reach into Foreign Companies*, WASH. POST, Jan. 28 2018, https://www.washingtonpost.com/world/asia_pacific/command-and-control-chinas-communist-party-extends-reach-into-foreign-companies/2018/01/28/cd49ffa6-fc57-11e7-9b5d-bbf0da31214d_story.html.

¹⁷⁷ *China’s Listed Firms Need to Beef Up Communist Party-building Activity, Regulator Says*, REUTERS, June 15, 2018, <https://www.reuters.com/article/us-china-governance-party/chinas-listed-firms-need-to-beef-up-communist-party-building-activity-regulator-says-idUSKBN1JB16F>.

include private companies.¹⁷⁸ For example Chinese regulators proposed last year that the government be allowed to take one percent stakes in major Chinese internet companies, allowing them a direct role in corporate decisions.¹⁷⁹ In short, even “private” Chinese companies receive high-level strategic direction from the Party.

The facts above provide a small glimpse into macro-level security concerns with respect to China, especially with regard to telecommunications. Since cyberespionage and related sabotage capabilities are conducted through telecom networks, it is not surprising that there should be a heightened focus on the risks associated with its communications infrastructure providers – especially those with large and broad market reach such as Huawei and ZTE.

C. Huawei and ZTE Have Particularly Close Ties to the Chinese State.

If China’s government intended to execute cyberespionage or sabotage operations against the United States, then Huawei and ZTE would be far more conducive to facilitating such an operation than would other companies. The government would enjoy obvious human and organizational advantages for such operations with these two large companies, as compared to

¹⁷⁸ See generally Ryan McMorro, *Business Leaders Bow To Xi As Communist Party Pushes In*, AGENCE-FRANCE PRESSE, Oct. 29, 2017, <https://www.japantimes.co.jp/news/2017/10/29/business/business-leaders-bow-xi-communist-party-pushes/>. According to a technology consultant, “[k]ey technology used to be controlled by state-owned companies and the party focused on those companies,” but “as private enterprise has grown stronger and become heavily woven into society, there is greater desire by the party to be involved.” *Id.* (quoting Mark Natkin, managing director at technology consultancy Marbridge Consulting). Per the article, the Party has already moved to strengthen control at state-owned enterprises, with dozens of publicly traded companies in Hong Kong rewriting their business charters this year to formalize the shift. For example, Guangzhou Automobile Group revised its business charter last July: “The CCP constitution was written into the document, according to filings. Major board decisions are now made after first consulting the company’s party committee.” *Id.*

¹⁷⁹ Li Yuan, *Beijing Pushes for a Direct Hand in China’s Big Tech Firms*, WALL ST. J., Oct. 11, 2017, <https://www.wsj.com/articles/beijing-pushes-for-a-direct-hand-in-chinas-big-tech-firms-1507758314>.

other non-China-based competitors. Put simply, Chinese government spies and would-be saboteurs would of course prefer to work with Chinese-speaking Chinese nationals who are employees of a Chinese communications company with Chinese supply chains and engineers, rather than a company with characteristics less suitable for clandestine espionage operations.

There are several specific aspects of Huawei and ZTE that are relevant to the national security aspects of this proceeding: (1) Huawei and ZTE are both headquartered in China and employ high-level managers who lead their internal CCP apparatus and are quoted in the press speaking in their CCP role on behalf of the companies; (2) both companies accept billions of dollars in state-backed funding to aid their international expansion; (3) Huawei and ZTE alike benefit from strategic state industrial development plans; and (4) they are positioned as potential conduits to channel advanced commercial technologies into China's military.

Party Committees within the companies. Huawei describes its ownership structure and notes that its Board "is currently comprised of 17 members, all of whom are private citizens who hold no positions in the Chinese government."¹⁸⁰ However, its leadership includes members of the CCP which claims ultimate authority in China and indeed directs matters of state.

The political relationship between the company and the Party is fundamentally different from the various partisan affiliations or activities that U.S. executives might undertake alongside, or even as part of, their corporate roles. In the U.S. system of government, even the most passionate partisan affiliations are legally distinct from business or governing. In contrast, the Party's pre-eminent role in China's society, ranking above government, is an essential and

¹⁸⁰ Huawei Comments, Ex. C, Dowding Decl. ¶ 16; *see also id.* ¶¶ 10-17 (describing ownership structure more generally).

foundational principle of the Chinese Constitution.¹⁸¹ In 1992 the CCP called for the establishment of a Party organization in all companies with three or more Party members, and the PRC Company Law now contains that requirement, as Huawei itself observes.¹⁸² Huawei maintains its own internal Party apparatus that is led by the company's Party Committee Secretary Zhou Daiqi. Zhou, who has worked at the company since 1994,¹⁸³ claims several senior operational roles at Huawei separate from his Party role, including as chief ethics and compliance officer and director of the corporate committee of ethics and compliance.¹⁸⁴

Zhou is identified in the press by his affiliation as Party Committee Secretary while promoting Huawei's business development and serving as a spokesperson for Huawei in the Chinese press. Numerous reports document Zhou's meetings on Huawei's behalf with other high-level Party and Chinese government dignitaries; he is always identified as Party Secretary,

¹⁸¹ Constitution of the People's Republic of China, Preamble, http://www.npc.gov.cn/englishnpc/Constitution/2007-11/15/content_1372962.htm ("The victory in China's New-Democratic Revolution and the successes in its socialist cause have been achieved by the Chinese people of all nationalities, *under the leadership of the Communist Party of China*.... *** *Under the leadership of the Communist Party of China* and the guidance of Marxism-Leninism, Mao Zedong Thought, Deng Xiaoping Theory and the important thought of Three Represents, the Chinese people of all nationalities will continue to adhere to the people's democratic dictatorship and the socialist road.... *** The system of the multi-party cooperation and political consultation *led by the Communist Party of China* will exist and develop for a long time to come.") (emphasis added).

¹⁸² Huawei Comments, Ex. D, Ye Decl. ¶ 14 ("It is true that the CCP sets up organizations within private enterprises and companies ... in accordance with PRC Company Law."); *id.* ¶ 28 (citing CCP's Bylaw, Article 30(1) and PRC Company Law art. 19).

¹⁸³ Huawei Investment & Holding Co., Ltd. 2017 Annual Report, at 118, Mar. 30, 2018, ("Huawei 2017 Annual Report"), http://www-file.huawei.com/-/media/CORPORATE/PDF/annual-report/annual_report2017_en.pdf.

¹⁸⁴ *Id.* at 118.

and only occasionally is his operational title as senior vice president mentioned afterwards.¹⁸⁵ In addition, Zhou has served as a top-level spokesperson on Huawei’s corporate strategy – describing to the press, for example, Huawei’s decisions to reach cross-licensing agreements on IPR to allow for faster market expansion and to establish global research institutes.¹⁸⁶

Importantly, while Zhou is mentioned in Huawei’s public annual report, the report omits the title of Party Committee Secretary that is used by the Chinese press. He is referred to instead by the less provocative title of executive member of Huawei’s ten-person supervisory board.¹⁸⁷ The supervisory board’s duties, according to Huawei’s annual report, are to ensure that members of the board fulfill their responsibilities, monitor the company’s operational and financial status, and to supervise internal controls and legal compliance.¹⁸⁸

Undoubtedly many other managers at Huawei participate in its internal Party Committee and other Party organizations in addition to fulfilling their corporate roles. As the company does

¹⁸⁵ See, e.g., *Ma Pingchang Visited Huawei, ZTE and Other Enterprises To Promote Key Information Industry Projects*, Baidu News, May 6, 2018, <https://www.kanzhun.com/news/306152.html> (describing “Huawei’s party secretary and senior vice president Zhou Daiqi” meeting with a visiting Party Secretary); *Wang Junzheng, Member of the Provincial Party Standing Committee and Secretary of the Municipal Party Committee, Met With Zhou Daiqi, Party Committee Secretary of Huawei Corp.*, TONGXINREN JIAYUAN (“Communications Homeland”), Mar. 2, 2016, <http://www.txrjy.com/thread-880470-1-1.html> (covering Zhou’s visit to the city of Changchun in Jilin province to meet with local Party and government officials, and describing him as “Party Secretary of Huawei Corporation”); *Wang Jianping Meets with Huawei’s Party Committee Secretary Zhou Daiqi*, CHINA GEZHOUBA REAL ESTATE: ENERGY CHINA NEWS, Aug. 23, 2017, <http://www.gzbfdc.com/news.aspx?type=10&id=6827> (describing Zhou’s meeting with a counterpart Party Secretary from a Beijing-based energy and construction conglomerate to discuss how Huawei could promote the use of its technology products in the energy industry).

¹⁸⁶ *Party Committee Secretary Zhou Daiqi: Internationalization Pushes Enterprises to Enhance Their Competitiveness*, SHENZHEN SPECIAL ECONOMIC ZONE ONLINE, Nov. 23, 2011, http://tech.southcn.com/t/2011-11/23/content_33696313.htm.

¹⁸⁷ Huawei 2017 Annual Report at 113.

¹⁸⁸ *Id.*

not make such numbers public, it is impossible to know how wide that network may be. But given the company's 180,000-person global payroll,¹⁸⁹ presumably the numbers are significant. In short, the CCP plays a critical role within Huawei's elite leadership and is in a position to exert influence over its personnel appointments and operations.

The situation is similar at ZTE. The company's Party Committee Secretary, Fan Qingfeng, was replaced at the end of May 2018, shortly after the United States blocked sales of American technology components to ZTE.¹⁹⁰ While still at ZTE, Fan was described in the Chinese press as meeting with Chinese officials in his Party capacity on behalf of the company, similar to his counterpart at Huawei.¹⁹¹ Also like Huawei's head Party officer, he was quoted in the domestic press outlining ZTE's corporate goals using his Party affiliation first and corporate title (senior vice president) second.¹⁹² But unlike his counterpart at Huawei, Fan also acted in a direct political role outside the company, serving in 2018 as a delegate to China's National People's Congress, the national legislative body.¹⁹³ Meanwhile, ZTE's incoming Party head

¹⁸⁹ *Id.* at 131.

¹⁹⁰ *ZTE to Replace Top Exec as China Seeks to Lift U.S. Ban*, BLOOMBERG NEWS, May 31, 2018, <https://www.bloomberg.com/news/articles/2018-05-31/zte-is-said-to-replace-top-exec-as-china-seeks-to-lift-u-s-ban>. Fan's firing was interpreted as a possible sign that China supported bringing in new leaders at ZTE, after the company had failed to abide by commitments for improved governance following serious export controls violations. *Id.*

¹⁹¹ *Luo Qiang Meets with ZTE Party Committee Secretary and Senior Vice President Fan Qingfeng*, CHENGDU DAILY, Nov. 6, 2017, <http://www.cdxfang.gov.cn/news/899.html> (describing a meeting with the Mayor of Chengdu in Sichuan Province).

¹⁹² *ZTE Secretary of the Party Committee: Strive to Produce 5G Equipment in the First Half of Next Year*, SECURITIES TIMES, Mar. 7, 2018, <http://finance.sina.com.cn/chanjing/gsnews/2018-03-07/doc-ifyaqryp6363520.shtml>; ZTE, Annual Report 2017, at 120, <https://res-www.zte.com.cn/mediare/zte/Investor/20180326/E1.pdf> ("ZTE 2017 Annual Report").

¹⁹³ *The Two Sessions Are Open; Who Are the 8 New Delegates to the National People's Congress in Shenzhen?*, SHENZHEN SPECIAL [ECONOMIC] ZONE, Mar. 3, 2018, http://www.sohu.com/a/224777875_321029.

Tian Dongfang was previously director of the Xi'an Microelectronic Technology Research Institute, an organization that claims it has made important contributions to both the Chinese domestic space industry and “the modernization of national defense.”¹⁹⁴ In sum, ZTE – like Huawei – has active Party involvement, with its most recent Party leader apparently involved in important corporate decision-making. Further underscoring ZTE’s ties to the state, its new slate of board members was handpicked by the company’s state-backed controlling shareholder.¹⁹⁵

Large subsidies. Huawei and ZTE are beneficiaries of multiple Chinese state policies that designate the development of the Chinese telecom sector as a strategic priority, and have received extensive government support over the years in the form of credit lines, export credits, grants, subsidies, and preferential tax treatment. It is beyond the scope of this filing to fully describe the enormity and the extent of such aid, which has been well-documented in recent

¹⁹⁴ *Tian Dongfang Was Appointed Secretary of the Party Committee of ZTE Corporation; Fan Qingfeng Was Dismissed*, SINA FINANCE, May 31, 2018, <http://finance.sina.com.cn/7x24/2018-05-31/doc-ihcikcev6481164.shtml>; ZTE 2017 Annual Report at 114; Xi'an Microelectronic Technology Research Institute (Aerospace 771 Institute) Work Unit Introduction, <http://www.modedu.cn/school/xawdz/index.htm> (visited June 13, 2018) (建所五十一年来取得了一系列重大科研成果...[包括]为我国航天事业的腾飞和国防现代化建设作出了重要贡献 “In the 51 years since its founding, the institute has achieved a series of major scientific achievements including ... [making] important contributions to the take-off of China’s space industry and the modernization of national defense.”).

¹⁹⁵ On June 29, 2018, ZTE replaced its entire board of directors, but the new board preserves the existing power structure and role of the Chinese state. See Dan Strumpf, Wenxin Fan & Kate O’Keefe, *ZTE Replaces Board, but Power Structure Remains*, WALL ST. J., June 29, 2018 (“All 14 directors, including Chairman Yin Yimin, resigned from ZTE’s board. The company named eight new directors as part of an overhaul that includes the firing of dozens of top executives. The incoming board members, however, were handpicked by ZTE’s state-backed controlling shareholder, filings show, and the majority are veteran officials of the shareholder or its state-backed parent companies.”).

years.¹⁹⁶ However, we provide some brief examples to highlight how both companies benefit from preferential financial treatment by the Chinese state.

Perhaps most significantly, China's export credit agencies have offered very significant financial support in recent years for Huawei and ZTE. As then-chairman and president of the Export-Import Bank of the United States Fred Hochberg explained in a speech:

[O]ne of the central reasons [Huawei's] growth has been so dramatic – is that it's backed by a \$30 billion credit line from the [state-backed] Chinese Development Bank. This backing allows Huawei to significantly reduce its cost of capital and to offer financing to their buyers at rates and terms that are better than their competitors. *** The reality is opaque state-directed capital allows foreign governments to target their financing at specific sectors and companies, while aggressively grabbing market share in an attempt to dominate a market. Companies like [U.S. telecom infrastructure firms] Patton and Cisco don't have access to \$30 billion to offset this market distortion.¹⁹⁷

The Chinese Development Bank (“CDB”) has been identified as one of the key reasons for Huawei's international success because it has provided such generous financing to help international customers buy equipment.¹⁹⁸ In their 2013 book on the CDB, authors Henry Sanderson and Michael Forsythe concluded that “[t]his gives Huawei and cross-town rival ZTE

¹⁹⁶ See generally Michael O. McCarthy, Chief Legal & Administrative Officer, Infinera Corporation, *Chinese Government Subsidies to the Optical Network Equipment Industry: Background Material for US-China Economic and Security Review Commission*, June 6, 2012, <https://www.uscc.gov/sites/default/files/6.14.12McCarthy.pdf>. Huawei also receives direct cash infusions from the government. In its 2017 annual report, the company said it had received government grants of 671 million yuan (\$105 million) for “its contributions to the development of research and innovation in the PRC.” Huawei 2017 Annual Report at 82. Also in 2017, Huawei received a separate grant of 326 million yuan (\$50 million) contingent on its completing “certain research and development projects.” Huawei 2017 Annual Report at 82.

¹⁹⁷ Fred Hochberg, Chairman and President of the Export-Import Bank of the United States, *How the U.S. Can Lead the World in Exports: Retooling Our Export Finance Strategy for the 21st Century*, Remarks at the Center for American Progress, June 15, 2011, https://www.exim.gov/sites/default/files/newsreleases/CAP_Speech.pdf (emphasis added).

¹⁹⁸ Henry Sanderson & Michael Forsythe, *Debt, Oil and Influence – How China Development Bank Is Rewriting the Rules of Finance: China's Superbank*, John Wiley & Sons, at 158 (2013).

Corp., with its own \$15 billion credit line from CDB, the means to provide competitive loans to lure customers away from Ericsson and Alcatel-Lucent.”¹⁹⁹ The authors took note of CDB’s unique “status as a state-owned bank that can raise large amounts of funds cheaply on the bond market: No other bank can compete with its scale until CDB commercializes and raises money on its own merit rather than that of the sovereign. *** Only when CDB pays the proper price to get money and China liberalizes interest rates will it start to price its giant loans at a market-based rate.”²⁰⁰

For example, in 2014-15, the CDB provided \$1.2 billion in funding for the purchase of equipment to modernize a mobile network in Brazil and \$600 million in loan assistance for Russia to undertake network upgrades.²⁰¹ Another state-backed institution, the Export-Import Bank of China (“China Exim Bank”), made available \$214 million for the acquisition of Huawei fiber-optic network gear in Guinea.²⁰² During this period, China’s government and export credit houses also provided financing and loans to promote the purchase of Huawei equipment for projects in Mali, Russia, Togo, Ukraine, and Zimbabwe.²⁰³ For ZTE during the same period, China Exim Bank provided \$154 million to finance a National Data Center in Bangladesh and

¹⁹⁹ *Id.*

²⁰⁰ *Id.* at 162.

²⁰¹ Export-Import Bank of the United States, *Competitiveness Reports - China Information*, at 9, June 30, 2016, https://www.exim.gov/sites/default/files/reports/competitiveness_reports/2015-2-2014%2B2015-China-Information.pdf (table showing \$1.2 billion project for Huawei in Brazil); *id.* at 30 (MegaFon in Russia takes out \$600 million loan from CDB for Huawei kit).

²⁰² *Id.* at 16 (\$214 million project in Guinea).

²⁰³ *Id.* at 23 (China loans Mali \$82 million for Huawei fiber network); *id.* at 29 (200 million yuan [\$30 million] from CDB for MTS in Russia); *id.* at 33 (\$25 million from China Exim Bank for Togo project with Huawei); *id.* at 34 (Ukraine telecom firm gets \$50 million from CDB for Huawei purchase); *id.* at 36 (China Exim Bank releases \$65 million for NetOne Zimbabwe re: Huawei).

the CDB made available \$500 million in loans for network equipment in Zimbabwe, Lesotho, and Burundi.²⁰⁴

An earlier European Commission (“EC”) report, published in 2011, concluded that Huawei had received “massive” credit lines from China’s export credit agencies.²⁰⁵ The EC’s investigation, which was never publicly released, said ZTE had access to credit lines “of an enormous magnitude” relative to its annual sales.²⁰⁶ For example, in 2009, ZTE’s credit lines amounted to \$25 billion on company revenue of \$8 billion.²⁰⁷ The Commission also found Huawei had access to a \$30 billion facility from CDB and that Huawei’s customers had used over \$5 billion in export buyer credits in the five-year period through 2009.²⁰⁸

In sum, various forms of commercially significant state aid and financing have directly contributed to Huawei’s and ZTE’s expansion, both domestically and globally.²⁰⁹

²⁰⁴ *Id.* at 4 (\$154 million from China Exim Bank to Bangladesh for ZTE project); *id.* at 9 (\$500 million for Econet Zimbabwe project in Zimbabwe, Lesotho, and Burundi).

²⁰⁵ Matthew Dalton, *EU Finds China Gives Aid to Huawei, ZTE*, WALL ST. J., Feb. 3, 2011, <https://www.wsj.com/articles/SB10001424052748703960804576120012288591074>.

²⁰⁶ *Id.*

²⁰⁷ *Id.*

²⁰⁸ *Id.*

²⁰⁹ These facts also undercut arguments by Huawei and other commenters who devote significant effort to examining and explaining the economic benefits of additional competition. Huawei Comments at 58-59; CCA Comments at 31-32; ITTA Comments at 5-6; *see generally* Huawei Comments, Ex. D, Shampine Decl. “The harm done by these subsidies to foreign competitors is ably chronicled ... Rivals are forced to go up against national champions that enjoy subsidised inputs and seemingly free money in markets that are protected. *** Such distortions breed indiscipline and overcapacity.” *Perverse Advantage*, THE ECONOMIST, Apr. 27, 2013, <https://www.economist.com/finance-and-economics/2013/04/27/perverse-advantage> (discussing Usha Haley and George Haley, “Subsidies to Chinese Industry,” Oxford University Press, Apr. 2013). If anything, Huawei’s presence in the market harms genuine free-market competition and hurts innovation by driving legitimate competitors out of business on the strength of its unfair advantages.

Standard-bearers for China's global network goals. China has positioned the overseas expansion of domestic telecom equipment providers as a national priority. A high-level memo issued in 2016 by the CCP's Central Committee and the State Council outlines plans to “formulate an overall plan for China's global network facilities construction, support businesses to tap into oversea markets and increase China's influence in global networks.”²¹⁰ The document set ambitious goals for Chinese telecom infrastructure expansion into geographies including Africa, south Asia, Russia, and Europe.²¹¹ Along similar lines, a 2017 plan outlining China's goals in cyberspace says the government “will promote information infrastructure connectivity and the Belt and Road Initiative with neighboring countries and beyond...”²¹² ZTE's then-Party Committee Secretary Fan echoed that call in a March 2018 interview that took place at the National People's Congress, urging more government support for network construction in Belt and Road countries.²¹³

Huawei and ZTE are China's biggest and most sophisticated network infrastructure firms. Boasting respective annual revenues of \$92.5 billion and \$17.2 billion, and with sophisticated technology portfolios and R&D capabilities, they serve as fitting channels for China to project its

²¹⁰ General Office of the CPC (Communist Party of China) Central Committee and State Council, *Outline of National Informatization Development Strategy* § 19, July 27, 2016.

²¹¹ *Id.* (“We should speed up the connection of China's information infrastructure with those of neighboring countries, create a corridor from Central Asia to West Africa, from South Asia to Indian Ocean, and from Russia to Middle East and Eastern European countries. We should also actively press ahead with the submarine cable construction projects reaching out to America, Europe and Africa. We should cooperate with relevant parties in building a China-Central Asia Information Platform, China-Asian Information Hub and Sino-Arabic Online Silk Road.”).

²¹² Ministry of Foreign Affairs and Cyberspace Administration of China, *International Strategy of Cooperation on Cyberspace*, Mar. 1, 2017.

²¹³ *The Information Economy Can Boost the 'One Belt and One Road,'* CHINA ECONOMIC NETWORK, Mar. 8, 2018, <http://news.sina.com.cn/c/2018-03-08/doc-ifynfhpq2510080.shtml>.

global digital ambitions.²¹⁴ While they are expected to accept and implement the Chinese state's international strategy, they also stand to reap the associated commercial benefits.

Conduits to channel advanced technology to China's military. China is engaged in a major initiative to promote the integration of advanced civilian technologies into the military sphere. In a speech in April 2018, President Xi articulated the need for policymakers to focus on "civil-military integration" amid the ongoing build-up of China's cyber capabilities.²¹⁵ That includes the military adoption of sophisticated technologies such as artificial intelligence, an area where Chinese advances are now challenging U.S. dominance in the field.²¹⁶ A 2017 Chinese government plan for the development of artificial intelligence calls for the "sharing of military and civilian innovation resources" and "form[ing] a new development pattern of deep integration of military and civilian [knowledge]."²¹⁷ The plan calls for channeling advanced innovations in artificial intelligence from the civilian side into China's defense sector, which it says will require

²¹⁴ Press Release, Huawei, *Huawei's 2017 Annual Report: Solid Performance and Lasting Value for Customers*, Mar. 30, 2018, <http://www.huawei.com/en/press-events/news/2018/3/Huawei-2017-Annual-Report>; *ZTE Reports Revenue Over 100 Bln Yuan in 2017*, XINHUA NEWS, Mar. 16, 2018, http://www.xinhuanet.com/english/2018-03/16/c_137043399.htm.

²¹⁵ Cyberspace Administration of China, *Xi Jinping: Indigenous Innovation Promotes the Development of Cyber Great Power Nation-states*, Apr. 21, 2018, http://www.cac.gov.cn/2018-04/21/c_1122719824.htm (quoting news story from Xinhua News).

²¹⁶ Julian E. Barnes & Josh Chin, *The New Arms Race in AI*, WALL ST. J., Mar. 2, 2018, <https://www.wsj.com/articles/the-new-arms-race-in-ai-1520009261> (describing an "escalating AI arms race," noting that "[o]ver the past two years, China has announced AI achievements that some U.S. officials fear could eclipse their own progress, at least in some military applications"). "This is our Sputnik moment," said Robert Work, the former deputy secretary of defense who oversaw the Pentagon's move into the new field. *** There should be no doubt that the Chinese military is chasing transformative AI technologies, said retired PLA Maj. Gen. Xu Guangyu, now a senior researcher at the China Arms Control and Disarmament Association, a government-supported think tank." *Id.*

²¹⁷ Chinese Communist Party Central Committee and State Council, *New Generation Artificial Intelligence Development Plan*, at sec. II, July 2017.

enhanced coordination among research institutes, colleges and universities, enterprises and military units.²¹⁸ The AI-specific initiative was reinforced by the release of a State Council plan in 2017 to create a more general national technology transfer system in China, in part to strengthen military-civilian coordination.²¹⁹

As flagship Chinese technology companies, Huawei and ZTE are well-positioned to assist these efforts. For example, Huawei's priority research areas include artificial intelligence, as well as 5G, cloud computing and IoT.²²⁰ The company maintains seven R&D shops in the United States and has invested about \$10 million per year in research and collaboration programs with various U.S. universities,²²¹ and supports another 18 R&D centers in Europe.²²² ZTE has formed the ZTE Forum for Cooperation of Enterprises, Academies and Research Institutes in order "to solicit memberships among leading domestic colleges and research institutes specialising in telecommunications technologies, in support of the government's call for the formation of a regime for cooperation in technological innovation[.]"²²³ ZTE claims five R&D

²¹⁸ *Id.* at sec. IV ("We will ... establish regular communication and coordination mechanisms among research institutes, colleges and universities, enterprises and military units.").

²¹⁹ State Council, *Notification of the National Technology Transfer System Construction Plan*, No. 44, Sept. 15, 2017, http://www.gov.cn/zhengce/content/2017-09/26/content_5227667.htm.

²²⁰ Huawei 2017 Annual Report at 12.

²²¹ Huawei, *Who We Are: History of Huawei's U.S. Operations*, <http://usahuawei.com/who-we-are/history-of-huaweis/> (visited June 26, 2018) (describing seven R&D centers developing the next generation of communications technologies, including our flagship research and development (R&D) facility in Santa Clara, California and investment of about \$10 million per year in research and collaboration programs with U.S. universities).

²²² Huawei Europe, *About Huawei*, <https://www.huawei.eu/about-huawei> (visited June 26, 2018) (scroll down to section on "The Company," describing 18 R&D organizations in eight European countries).

²²³ ZTE 2017 Annual Report at 27.

centers in the United States plus another fifteen spread across China, Sweden, France, Japan and Canada.²²⁴

Huawei and ZTE also have top leadership with ties to the Chinese military. As noted earlier, ZTE's incoming Party Committee Chairman most recently worked at a research institute that boasts of its contributions to the modernization of China's national defense. Given their sophisticated global R&D facilities and research partnerships, Huawei and ZTE are in a position to serve as important conduits for Beijing to acquire and assimilate technical knowledge.

In summary, Huawei and ZTE serve as far more than mere commercial actors in the ICT industry. While the primary aim of U.S. firms is to maximize profit for shareholders, the record suggests that Huawei and ZTE are obliged to not only seek profits, but also to further the interests of the Chinese state. The two companies take directives from the Chinese Communist Party, which closely oversees and supports their development, and allow top officials in its Party apparatus to speak on their behalf. They benefit from very significant amounts of Chinese government financial help and from industrial plans that facilitate their entry into foreign markets around the world. And they are in a position to acquire and generate advanced technologies of considerable value to the Chinese military.

D. Huawei's Statements Regarding Its Corporate Conduct Are Immaterial in the Proceeding at Hand.

Huawei's effort at self-defense in its comments in this proceeding relies on facts and arguments that are irrelevant. In its comments, Huawei has submitted cybersecurity white papers

²²⁴ ZTE USA, *About Us*, <https://www.zteusa.com/about-us-old> (visited June 16, 2018); ZTE 2017 Annual Report at 26 ("We have established 20 R&D centres in China, the United States, Sweden, France, Japan and Canada, as well as more than 10 joint innovation centres established in association with leading carriers to ensure success in the market through better assessment of market demand and customers' experience.").

and internal corporate materials such as information about its corporate governance structure, employee guidelines for business conduct, and employee filings in order to attest to the company’s good intentions and to argue that it does not present a national security risk.²²⁵ In light of the larger security concerns we have outlined, these submissions have no bearing on the Commission’s consideration in this proceeding, as they are all subordinate to direction from the Chinese state or the CCP.

Huawei and ZTE benefit from and ultimately answer to the CCP – which, as previously established, maintains supreme authority within the Chinese state according to the nation’s Constitution. Huawei and ZTE may possess some of the trappings of a “normal” multinational company, but that does not change the essential fact that these companies and their employees and activities are in a subordinate position to the Communist Party, which has an increasingly adversarial relationship to the United States. Given the national security context, the supporting materials Huawei has provided are immaterial to the questions raised in the FCC proceeding. The relevant issue is that Huawei and ZTE are beholden to an institution – the Party – under whose guidance China seems inclined to act in ways counter to the interests of the United States.

V. COMMENTERS THAT OPPOSE COMMISSION ACTION FAIL TO IDENTIFY CREDIBLE LEGAL BARRIERS TO THE ADOPTION OF A NARROWLY TAILORED RULE IN THIS CONTEXT.

A few parties – CCA and Huawei most prominently – raise a host of legal challenges to the adoption of seemingly *any* rule in this proceeding.²²⁶ Their assorted arguments do not pose

²²⁵ Huawei Comments at 86-91; *see generally id.*, Ex. A, Suffolk Decl. at 6 (“I can confirm that I have never been unduly influenced . . .”); *id.*, Ex. B, Purdy Decl. ¶ 42 (same); *id.*, Ex. C, Dowding Decl. at Ex. 1 (attaching employee business conduct guidelines); *id.*, Exs. I to L (four cybersecurity white papers); *id.*, Ex. O, Certification and Testing of Huawei Products (attaching various certifications).

²²⁶ *See, e.g.*, Huawei Comments at 13-35; CCA Comments at 15-27; ITTA Comments at 7-9.

any obstacles to the sort of targeted action that the Commission has proposed and that a majority of commenters support. A narrowly tailored rule like that favored by TIA and many other parties is squarely within the Commission’s universal service authority to ensure high-quality, reliable service and to protect rural and low-income consumers against inferior networks and services. Moreover, the process by which the Commission has proposed to develop and implement such a rule is consistent with the APA and established agency practice. Finally, a narrow USF-related restriction as contemplated in this proceeding raises no constitutional concerns whatsoever. Huawei’s and CCA’s claims to the contrary dramatically overstate and mischaracterize the limited action the Commission proposes to take.

A. The Communications Act Provides the Commission with Sufficient Statutory Authority to Adopt a Targeted USF Restriction.

The record confirms that the Commission has clear legal authority under the Act to take targeted and specific action to promote national security interests in the universal service context.²²⁷ As TIA discussed in its initial comments, the Commission has a unique responsibility and ability to ensure that the funds it makes available to USF recipients are not utilized in a way that would pose a risk to national security.²²⁸

1. The Commission’s Adoption of a Targeted USF Restriction Is Rooted Squarely In Its Universal Service Authority.

The Commission’s authority to impose conditions on the use of USF support – and particularly on the facilities that are deployed using such support – is well established. As TIA discussed in its initial comments, in upholding the Commission’s *USF/ICC Transformation*

²²⁷ See, e.g., USTelecom Comments at 16; NCTA Comments at 17; EchoStar/Hughes Comments at 7.

²²⁸ TIA Comments at 5-6.

Order, the Tenth Circuit specifically upheld the Commission’s authority to impose the condition on the receipt of USF funds to provide broadband service in addition to the supported service to advance the Commission’s legitimate universal service goals.²²⁹

Opponents of Commission action attempt to argue that “national security” is not one of the enumerated Section 254(b) goals,²³⁰ but this is just a strawman. In fact, a targeted rule here would clearly advance the Commission’s responsibilities under Section 254(b), as discussed below. Parties opposing a rule here also argue that identifying national security threats is not within this Commission’s legal purview.²³¹ Yet, TIA and other commenters make clear that any Commission rule should flow from, and be coordinated with, broader U.S. government actions led by the agencies specifically charged with protecting national security, such as DHS.²³² TIA and other parties supporting targeted action here do not propose or support expansion of the FCC into the national security arena; rather, we simply support the Commission’s recognition of other appropriate agencies’ identification of network threats, and use of that information to advance the Commission’s legitimate universal service objectives.²³³ Nothing in the Communications Act prevents the FCC from coordinating with and relying on information provided by other federal agencies as an input into its universal service decision-making process.

²²⁹ *Id.* at 23-24 (citing *Direct Communs. Cedar Valley, LLC v. FCC (In re FCC 11-161)*, 753 F.3d 1015, 1046 (10th Cir. 2014)).

²³⁰ *See, e.g.*, Huawei Comments at 12-24; CCA Comments at 5, 15-16, 25.

²³¹ Huawei Comments at 12-24; CCA Comments at 5, 12-22.

²³² *See, e.g.*, TIA Comments at 28-60; CTIA Comments at 13-16; EchoStar/Hughes Comments at 7-8; Motorola Comments at 4; NCTA Comments at 6-10; USTelecom Comments at 3-5.

²³³ TIA Comments at 28-60; CTIA Comments at 13-16.

At the same time, however, TIA has urged the Commission to identify and observe strict limiting principles on its use of that authority.²³⁴ The Commission should not become a unilateral arbiter of when national security is threatened, but should instead rely upon assessments and determinations made by Congress, the President or agencies with appropriate expertise regarding certain suppliers, and apply those decisions in its independent USF oversight capacity. In adopting its proposal, the Commission should eliminate any doubt about the scope of its intended action and make these self-imposed limits clear.

In launching a broadside against Commission authority in this context, parties opposing the Commission's proposal lose sight of the premise that any Commission action here would and should be quite narrow. These parties assume too readily that the Commission would be exercising its legal authority to "make" national security decisions.²³⁵ The Notice, however, contemplates a surgical strike through a valid exercise of the Commission's judicially affirmed authority to impose conditions on federal subsidies under Section 254 of the Act.²³⁶ As the Commission has correctly recognized, the USF is "a public-private partnership" and eligible telecommunications carriers "that benefit from public investment in their networks must be subject to clearly defined obligations associated with the use of such funding."²³⁷ Given the emerging consensus that government action is needed to mitigate the risk of state-sponsored

²³⁴ TIA Comments at 25-28.

²³⁵ See, e.g., Huawei Comments at 23.

²³⁶ See *Direct Communs. Cedar Valley*, 753 F.3d at 1046 (finding that "nothing in the statute limits the FCC's authority to place conditions ... on the use of USF funds"); see also *Qwest Communs. Int'l, Inc. v. FCC*, 398 F.3d 1222, 1238 (10th Cir. 2005) (stating that the Commission "is in a unique position to determine what inducements are necessary to effectuate the goals of the Act") (*Qwest II*).

²³⁷ *Connect America Fund*, Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd 17663 ¶ 74 (2011) (*Connect America R&O*).

cyberespionage efforts, a condition that prohibits USF dollars from being used on products from suppliers identified as posing national security risks is a common-sense approach that will ensure the continuing integrity of the fund.

Huawei and CCA also argue that the Commission’s interpretation of “public interest” must be read narrowly as it relates to USF principles as a whole, and does not encompass “national security,”²³⁸ but here, the “national security” concerns are potential sabotage and espionage, which pertain to the reliability and integrity of the networks – public interest concerns that fall squarely within the enumerated goals of Section 254(b). It is impossible to read “public interest” so narrowly as to exclude reliability and integrity of the networks that serve the public; without such networks, there can be no meaningful universal service. Thus, the principles of universal service presume national security.

In sum, the targeted rule that TIA and other commenters favor would clearly be in the public interest, and such action would be rooted squarely in the Commission’s universal service authority. It would not be grounded only in a “vague articulation of the ‘public interest’” which “cannot override the six specified principles in Section 254.”²³⁹ Rather than undermining the deployment of affordable service in rural areas, it would protect rural and low-income consumers against network disruptions and cyber threats. And rather than expanding the Commission’s authority into national security areas not clearly specified by statute, it would allow the Commission to utilize information developed by appropriate agencies with national security authority to advance the Commission’s core statutory obligation to protect the integrity of the nation’s communications networks.

²³⁸ See Huawei Comments at 26-27; CCA Comments at 25-26.

²³⁹ CCA Comments at 19.

2. Ensuring the Security of USF-Supported Networks is Consistent with the Universal Service Principles in Section 254(b) of the Act.

Section 254(b) of the Communications Act requires the Commission to base its universal service policies on a set of principles designed to ensure the “preservation and advancement of universal service.”²⁴⁰ Conditioning the availability of USF support to be available only for equipment and services that do not pose a risk to national security – as one element of a broader universal service regime with a potential impact on only a very small number of companies – is neither inconsistent with nor unrelated to the principles outlined in Section 254(b). Nor does the Commission need to establish a new universal service principle to effectuate its policy choice in this proceeding since its action is consistent with existing principles. Thus, arguments concerning the process required to establish a new universal service principle are irrelevant.²⁴¹

Commenters opposing Commission action are incorrect in asserting that “the Commission’s proposed restriction ... *thwarts* the achievement of the statutorily enumerated universal-service principles” in Section 254(b).²⁴² In fact, targeted action to eliminate dangerous equipment from USF-supported networks will advance the goals set out in Section 254(b). Arguments that the Commission lacks authority to promulgate targeted rules to protect the USF-supported supply chain all depend on a false choice, with every argument effectively stating that the Commission can *either* have affordable service and broadly deployed networks in rural areas using equipment from problematic suppliers, *or* less deployment (or even no deployment) and more-expensive service without such equipment.²⁴³

²⁴⁰ 47 U.S.C. § 254(b).

²⁴¹ Huawei Comments at 15; CCA Comments at 19.

²⁴² Huawei Comments at 16 (emphasis in original). *See also* CCA Comments at 16-24; ITTA Comments at 7-9.

²⁴³ *See, e.g.*, Huawei Comments at 12-35; CCA Comments at 15-27.

These arguments, however, ignore the fundamental premise that motivates this proceeding – the very real danger presented by certain equipment of harm to communications networks or the customers who use them. It is of no moment that service is extended to customers in a rural area if that network relies on equipment built by a problematic supplier that could bring the network down with the stroke of a key in a foreign capital, or compromise customer’ sensitive information, or facilitate espionage that puts those customers’ lives and property at risk. As TIA explained in its comments, U.S. Executive Branch and Congressional authorities have studied this issue carefully and concluded that equipment from certain manufacturers poses grave threats to U.S. networks.²⁴⁴ TIA, like the majority of commenters, supports targeted, specific action to prevent the expenditure of USF funding to purchase equipment that has been properly identified by the branches of government with expertise in this area.²⁴⁵

Commenters also overstate the potential harm from FCC action given the multitude of options available to all USF-supported companies for all equipment and services currently offered by Huawei and ZTE, *see* section III-C above, and the fact that it appears that a small number of companies would be impacted, *see* section III-B above. After stripping out the rhetoric, the facts boil down to these: the FCC is proposing to condition approximately \$9 billion in USF support on a policy that such funds not be available to purchase equipment that has been identified by expert national security entities as a national security risk and in so doing could potentially impact a small number of companies who currently receive a fraction of that support, each of whom have multiple additional choices available to them sufficient to meet their

²⁴⁴ TIA Comments at 9-18.

²⁴⁵ *Id.* at 4, 78-80.

USF obligations. Suggesting that is not the case belies the fact that hundreds of companies have been able to provide reasonably comparable service at reasonably comparable rates without reliance on Huawei or ZTE. The lens through which Section 254(b)'s principles are viewed must be based on this reality, not the doomsday scenario painted by some commenters.

Targeted action by the Commission in this proceeding, if properly implemented as proposed by TIA and other commenters, will advance, not undermine, the universal service principles articulated in Section 254(b). The Commission would ignore its obligation under Section 254(b)(1) to ensure the availability of “[q]uality services” if it allowed USF-funded networks to depend on equipment that has been identified by appropriate U.S. government agencies as posing a threat to reliability, security, or both. CTIA underscores this point when it states that “a security compromise that a nation-state intelligence service may have embedded in a certain supplier’s core network equipment could have broad implications for all users of that network – indeed, for the reliability of the network itself.”²⁴⁶ Consumers are unlikely to believe they are receiving “quality services” if those services are subject to disruption by foreign powers, or if a price of those services is the insecurity of their personal data, thereby jeopardizing the Commission’s goal of promoting “[a]ccess to advanced telecommunications and information services” under Section 254(b)(2).²⁴⁷

²⁴⁶ CTIA Comments at 16-17.

²⁴⁷ In *Qwest I*, the Tenth Circuit explained that while the Act imposes a “mandatory duty” on the Commission to “base its universal service policies on the principles listed in § 254(b),” each of those principles is phrased in terms of “should,” which indicates only “a recommended course of action.” Thus, if the Commission elects to promote quality services and access to advanced services in this proceeding, the other section 254(b) principles “can be trumped.” *Qwest Corp. v. FCC*, 258 F.3d 1191, 1200 (10th Cir. 2001) (“*Qwest I*”).

CCA expresses concerns that FCC action will violate the principle in Section 254(b)(1) that service be available at reasonable and affordable rates.²⁴⁸ It cannot be argued that eliminating the availability of equipment from two problematic vendors violates a broad principle when only a very small number of companies may be impacted. Given that hundreds of USF-companies have been able to provide quality services at reasonable and affordable rates using other suppliers, the claim rings hollow.²⁴⁹ With respect to any particular company that may be impacted, as TIA has suggested, the FCC should consider remedial measures as necessary to address such potential harms. But the impact on a handful of companies cannot be the basis for suggesting a violation of a broad principle.

Similarly, the Commission would ignore its obligations under Section 254(b)(3) to ensure that users of USF-funded networks, including “low-income consumers and those in rural, insular, and high-cost areas ... have access to telecommunications and information services ... that are reasonably comparable to those services provided in urban areas” if it allowed providers receiving funding to serve these customers to use dangerous equipment that is not used in networks in urban, wealthier areas. Opponents of Commission action argue that Huawei and ZTE equipment is necessary to properly serve rural and low-income customers because of these manufacturers’ lower costs and better responsiveness to rural carriers’ needs.²⁵⁰ In fact, relegating rural and low-income consumers to reliance on dangerous equipment from foreign suppliers prevents those consumers from receiving services that are “reasonably comparable” to

²⁴⁸ CCA Comments at 17.

²⁴⁹ These facts also counter claims that the proposed rule conflicts with the principles in Section 254(b)(2) (access to advanced services) and Section 254(b)(6) (access to advanced telecommunications services for schools, health care, and libraries).

²⁵⁰ *See, e.g.*, CCA Comments at 8.

those that urban and higher-income customers receive from nationwide carriers and other providers serving urban markets. For these same reasons, arguments that targeted Commission action against appropriately identified dangerous equipment would disproportionately impact small and rural carriers ring hollow. For example, CCA argues that the “proposed rule is directly contrary to the USF’s very purpose: supporting carriers that provide service to rural and low-density regions of the country.”²⁵¹

Relatedly, CCA argues that the proposed rule would violate the Commission-enacted principle of “competitive neutrality,” which generally holds that “universal service support mechanisms ... should not unfairly advantage nor disadvantage one provider over another, and neither unfairly favor nor disfavor one technology over another.”²⁵² A USF restriction as described in the record of this proceeding would not violate the principle of “competitive neutrality.” This principle does not protect individual competitors. It protects consumers by ensuring that the Commission does not favor one service provider or one service provider’s technology over that of another “so as to facilitate a market-based process whereby each user comes to be served by the most efficient technology and carrier.”²⁵³ The Commission’s proposal does not interfere in this market-based process. It simply would apply an across-the-board condition on receipt of universal service funds equally to all providers in furtherance of the universal service goals. As TIA has explained, adopting a rule comparable to that proposed in the *Notice* on a prospective basis would only impact a small segment of the marketplace.

²⁵¹ *Id.* at 36.

²⁵² *Federal-State Joint Board on Universal Service*, Report and Order, 12 FCC Rcd 8776, 8801 ¶ 47 (1997).

²⁵³ *Id.* at 8802 ¶ 48.

Further, as the courts have recognized, any concerns about “competitive neutrality” can be adequately addressed through waivers or additional funding on a case-by-case basis.²⁵⁴

Finally, for the Commission to focus on USF-supported networks, where its authority is clear, is in no way “an artificial narrowing of the scope of the regulatory problem.”²⁵⁵ The Commission is under no obligation to address every facet of a regulatory problem in a single rulemaking; indeed, given the questions that have been raised regarding the Commission’s authority outside the USF context and the lack of any indication in the record that the problematic equipment is used in networks in more urbanized parts of the U.S., its decision to tackle one element of the problem is admirable.²⁵⁶ It is, in short, entirely appropriate for the Commission initially to focus on one aspect of the problem that falls clearly within its statutory authority. In sum, a rule restricting the use of USF support to purchase equipment made by manufacturers identified by appropriate U.S. governmental agencies will advance, not thwart, the fundamental principles of universal service.

B. Adoption of a Narrowly Tailored Rule Would Not Be Arbitrary, Capricious, an Abuse of Discretion, or Otherwise Inconsistent with Law.

A few commenters argue that the adoption of a narrowly tailored rule similar to that proposed in the Notice would be inconsistent with established principles of administrative law.²⁵⁷ This is simply not the case. In pursuing such a measure, the Commission may rely on determinations made by agencies that possess national security expertise or by Congress.

²⁵⁴ See *Rural Cellular Ass’n v. FCC*, 588 F.3d 1095, 1105 (D.C. Cir. 2009) (noting the availability of additional funding as a mechanism to ameliorate any potentially “unfair” effects under the competitive neutrality principle).

²⁵⁵ CCA Comments at 35 (quoting *Home Box Office, Inc. v. FCC*, 567 F.2d 9, 36 (D.C. Cir. 1977)).

²⁵⁶ See, e.g., TIA Comments at 19.

²⁵⁷ Huawei Comments at 35-53, 75-83; CCA Comments at 47-48.

Further, arguments that the Notice is arbitrary and capricious because it does not propose solving all threats facing the supply chain are unpersuasive, as the Commission is well within its discretion to determine (and limit) the scope of its response to a particular problem; a rule similar to the one proposed in the Notice is rationally related to protecting supply chain security.

Finally, the Commission has complied with notice requirements under the APA.

1. The Commission May Permissibly Derive a List of Prohibited Suppliers from Determinations Made by Expert Agencies or by Congress.

Most parties in this proceeding agree that the Commission should not attempt to make national security determinations of its own, as such matters are outside of its core expertise; these parties thus support the reasonable alternative that the Commission should rely on the informed efforts of those in government that do possess the requisite national security knowledge, experience, and access to classified information.²⁵⁸ Although Huawei agrees with the limits on the Commission's capabilities in this context,²⁵⁹ it then argues implausibly that the Commission is foreclosed from seeking any guidance from other experts and that any effort to derive a list of prohibited suppliers from determinations that have already been vetted elsewhere is an impermissible "shortcut."²⁶⁰ Through several untenable theories, Huawei seeks to wedge the Commission between a rock and a hard place, such that it would be disabled from doing *anything* in this area.

Huawei's arguments ignore the nature of the relevant authority that the Commission does possess, as well as the way agencies of the government actually relate to and work with each

²⁵⁸ See *supra* sections I-A and II-C.

²⁵⁹ Huawei Comments at 20-21.

²⁶⁰ *Id.* at 75-86.

other. First, in looking to existing statutes such as the 2018 NDAA, the Commission would not be relying on them as authority for its own action or otherwise “expanding” that legislation.²⁶¹ Rather, the Commission would be acting on its own authority under the Communications Act, appropriately informing itself using the 2018 NDAA, among other sources.²⁶² Notably, Huawei’s expert, Professor Emily Hammond, bypasses this threshold inquiry in her report: She concedes that she did “not separately analyze[] whether the FCC [already] has statutory authority to determine whether companies pose national security threats in the context of administering the USF program,” before subsequently concluding that the Commission’s proposed actions would be “in excess” of its statutory mandate.²⁶³

Further, Huawei’s concerns about “subdelegation” mischaracterize the law and the nature of any Commission action here.²⁶⁴ Agencies routinely share insights as part of the cooperative administration of government without raising subdelegation concerns,²⁶⁵ so long as those

²⁶¹ *Id.* at 81-83.

²⁶² *See supra* section V-A.

²⁶³ *Compare* Huawei Comments, Ex. H, Hammond Decl. at 2 (“In preparing this report, I have not separately analyzed whether the FCC has statutory authority to determine whether companies pose national security threats in the context of administering the USF program.”), *with id.* at 15 (“Relying on Statutory or Other Lists Would Be ... in Excess of the FCC’s Statutory Mandate.”) (capitalization in original).

²⁶⁴ Huawei Comments at 81.

²⁶⁵ *See United States v. Matherson*, 367 F. Supp. 779, 782-83 (E.D.N.Y. 1973), *aff’d*, 493 F.2d 1339 (2d Cir. 1974) (“[A] federal agency entrusted with broad discretion to permit or forbid certain activities may condition its grant of permission on the decision of another entity, such as a state, local, or tribal government, so long as there is a reasonable connection between the outside entity’s decision and the federal agency’s determination.”).

agencies retain oversight and accountability over their final decision-making.²⁶⁶ Where, as here, statutes and agency determinations are merely evidence that inform and provide context for the Commission’s ultimate findings, the Commission cannot be said to be unlawfully delegating its authority to outside parties.²⁶⁷

As discussed above, the Commission has authority to take the narrow action it has proposed here and thus need not (and does not propose to) delegate the task of protecting the security of USF-funded networks to any other entity. And more generally, the Commission routinely consults agencies with national security expertise without yielding its ultimate decision-making role. Indeed, cooperative relationships of information-sharing among DHS, DOJ (including the Federal Bureau of Investigations), DOD, the Department of State, DOC and NTIA, the USTR, and the Office of Science and Technology Policy are formally integrated into the Commission’s procedures.²⁶⁸ These agencies are encouraged to review and submit recommendations to the Commission as to the risks affecting their respective subject-matter areas, and between 2013-2015, they participated in nearly one in five of all such applications that

²⁶⁶ See, e.g., *National Park & Conservation Ass’n v. Stanton*, 54 F. Supp. 2d 7 (D.D.C. 1999) (holding that the National Parks Service’s delegation of its statutory management duties to a private, independent council was an unlawful subdelegation because NPS retained no oversight over the council and no final reviewing authority over the council’s actions or inaction); *US Telecom Ass’n v. FCC*, 359 F.3d 554, 567 (D.C. Cir. 2004) (holding that the Commission’s subdelegation of “almost the entire determination of whether a specific statutory requirement ... has been satisfied” to state commissioners was unlawful).

²⁶⁷ Notice ¶ 20.

²⁶⁸ *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market; Market Entry and Regulation of Foreign-Affiliated Entities*, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23919 ¶ 63 (1997) (“*Foreign Participation Order*”); see also *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, Notice of Proposed Rulemaking, 31 FCC Rcd 7456, 7457-59 ¶¶ 4-8 & n.16 (2016) (“*Executive Branch Process Reform NPRM*”).

appeared before the Commission.²⁶⁹ Consistent with delegation principles, in those cases the Commission retains complete, independent authority in determining whether or not to grant any particular application.²⁷⁰ Huawei’s demeaning claim that citing determinations by these agencies in this context would reduce the Commission to “a ventriloquist’s puppet” completely ignores this established practice of inter-agency cooperation, not to mention the Commission’s own authority and expertise in this context.²⁷¹

Relatedly, the Commission regularly relies on adjudications of wrongdoing made in other arenas to inform its responsibilities under the Communications Act. Most notably, in the universal service context, the Commission pursues debarment against a USF participant based on a “conviction of or civil judgment for” fraud or abuse rendered elsewhere.²⁷² The Commission is not expected to re-litigate the matter, nor could it reasonably be expected to do so. While the debarment process is not otherwise relevant to the Commission’s proposed action here,²⁷³ that rule offers a useful analogy that informs and legitimizes the Commission’s intention to proceed based on security-related determinations made by expert agencies.

²⁶⁹ *Executive Branch Process Reform NPRM*, 31 FCC Rcd at 7457-58 ¶ 4; *see, e.g., Applications of LightSquared Subsidiary LLC, Debtor-in-Possession, and LightSquared Subsidiary LLC For Consent to Assign and Transfer Licenses*, Declaratory Ruling, 30 FCC Rcd 13988 (2015) (conditioning grant of Commission approval on the applicants’ compliance with obligations separately imposed by the national security agencies).

²⁷⁰ *See Executive Branch Process Reform NPRM*, 31 FCC Rcd at 7457-58 ¶ 4; *Foreign Participation Order*, 12 FCC Rcd at 23920-21 ¶¶ 65-66.

²⁷¹ Huawei Comments at 84.

²⁷² 47 C.F.R. § 54.8(c).

²⁷³ Although Huawei appears to suggest that the Notice’s proposal is a USF-related debarment governed by those specific procedures, Huawei Comments at 71-72, that process is substantively distinct from the one at issue here. And as discussed below, the procedural safeguards contemplated by that process are present here in any event.

There is no reason the Commission could not pursue a similar approach here. Pursuant to the proposals advanced in the opening round of comments, the Commission would solicit input regarding extant sources of congressional or agency expertise, but the Commission will independently enact the final rules of general applicability.²⁷⁴ At no point would the Commission be expected to shirk its statutory obligations and relinquish to Congress or others its authority to determine how USF funds are distributed. In this manner, determinations from outside parties may supplement the Commission's lawful and reasoned decision-making process without raising any issues of subdelegation. Although Huawei suggests the risk of a disconnect between another agency's determination and the Commission's USF-related goals in this proceeding,²⁷⁵ TIA has proposed limiting principles on what sort of collateral decisions should and should not guide the development of a list of prohibited suppliers.²⁷⁶

Finally, from a process standpoint, there is no legal barrier to the Commission developing a list of prohibited suppliers through this rulemaking. As discussed below, the Commission has discretion to proceed pursuant to a notice-and-comment rulemaking as opposed to an adjudication, and this rulemaking affords parties all of the procedural safeguards expected under the APA and due process, including an explanation of the bases for the Commission's proposed restriction, opportunities for a response, and a reasoned determination logically connecting the facts adduced with the choices made.²⁷⁷ In addition, because a USF-related restriction is a justifiable means of enhancing supply chain security as described elsewhere in these comments

²⁷⁴ Notice ¶¶ 14, 19-23.

²⁷⁵ Huawei Comments at 84-85.

²⁷⁶ TIA Comments at 55-58.

²⁷⁷ See *infra* section V-C-1.

and in TIA’s opening submission, any rule the Commission adopts will not have unreasonable “secondary retroactivity” and thus is not barred by the APA.²⁷⁸

2. The Commission Need Not Address All Supply Chain Security Issues at Once.

In its comments, Huawei argues that the Commission’s proposed rule would be arbitrary and capricious because it utilizes “irrational decisionmaking” and only applies to a few companies participating in the USF program, rather than the supply chain on a whole.²⁷⁹ Huawei further complains that the proposed rule leaves some national security questions unanswered.²⁸⁰ Contrary to these arguments, the Commission is fully justified in taking the narrow approach proposed in the Notice.

At the outset, TIA has advocated that a narrowly tailored rule comparable to the one proposed in the Notice would have a meaningful, positive impact on USF supply chain security. To that end, TIA first has urged the Commission to focus on issues regarding specific suppliers deemed to pose a national security threat, even as general supply chain security issues are being handled by industry and in partnership with other federal agencies.²⁸¹ As TIA has explained, there is ample record evidence to justify a focus at this time on the particular companies discussed in the Notice.²⁸² Next, the Commission is undoubtedly focused primarily on issues regarding federal funds disbursed through the USF program, even as the same security concerns

²⁷⁸ Huawei Comments at 80-81 (citing *U.S. Airwaves, Inc. v. FCC*, 232 F.3d 227, 233 (D.C. Cir. 2000)).

²⁷⁹ *Id.* at 51-52.

²⁸⁰ *See, e.g., id.* at 53 (“The Commission has focused on Chinese companies, even though companies with ties to other countries could pose similar or greater risks to national security.”).

²⁸¹ *See supra* sections II-B and II-C; *see also* TIA Comments at 28-34.

²⁸² *See supra* section IV-A; *see also* TIA Comments at 9-19.

would likely apply in other networks not funded through the USF program.²⁸³ Finally, the Commission has appropriately focused on specific problems related to cyberespionage or malicious disruption associated with a remote cyberattack, rather than other types of threat vectors that might require the actor to achieve some physical proximity to products during the distribution, installation, or operation phase.²⁸⁴

This narrow approach is permissible under longstanding principles of administrative law. That is, even if the Commission adopts a narrowly tailored rule focused on redressing certain specific problems while leaving other potential threats to the supply chain unanswered, the rule would not be arbitrary and capricious. Agencies are permitted to determine that incremental steps still serve a legitimate purpose and may act on a particular aspect of a problem while “neglecting the others.”²⁸⁵ When enacting a rule, administrative agencies must necessarily draw lines when deciding the class of persons affected by a regulation based on determinations within its expertise.²⁸⁶ They may approach an issue one step at a time, focusing on certain areas while ignoring others,²⁸⁷ and “the fact [that] the line might have been drawn differently at some points is a matter for legislative, rather than judicial, consideration.”²⁸⁸ Moreover, even under the

²⁸³ See *supra* section III-A.

²⁸⁴ See *id.* & n.78.

²⁸⁵ *FCC v. Beach Commc’ns*, 508 U.S. 307, 316 (1993) (citing *Williamson v. Lee Optical of Okla., Inc.*, 348 U.S. 483, 489 (1955)); see also *Kaemmerling v. Lappin*, 553 F.3d 669, 685-86 (D.C. Cir. 2008) (citing *Williamson*); *Am. Council of Life Insurers v. D.C. Health Benefit Exch. Auth.*, 73 F. Supp. 3d 65, 105-08 (D.D.C. 2014) (citing *Williamson*).

²⁸⁶ *Beach Commc’ns*, 508 U.S. at 316 (citing *Williamson*).

²⁸⁷ *Williamson*, 348 U.S. at 489.

²⁸⁸ *Beach Commc’ns* at 316.

deference typically afforded to agencies,²⁸⁹ a regulation need only to be rationally related to its legitimate purpose; it need not solve all relevant issues at once. Given this deference, the under-inclusiveness of an agency regulation alone does not make it unconstitutional, arbitrary, or capricious.²⁹⁰

Under these principles, the Commission is permitted to enact a narrowly tailored rule – one which would meaningfully benefit national security – without confronting every national security threat facing the telecommunications supply chain in one proceeding. While the adoption of a narrowly tailored rule would not purport to solve all of the national security threats facing the telecommunications supply chain, the Commission does not have to reach a regulatory conclusion that “all evils of the same genus be eradicated or none at all.”²⁹¹ On the contrary, the Commission would have engaged in rational decision-making given that it has a specific, supporting role to play, and a narrowly targeted restriction on USF funds would be consistent with that role and serve the public interest.

3. The Commission Has Provided Adequate Notice to Adopt Its Proposed Rule or Reasonable Variants Thereof.

Concerns expressed by a few commenters that the Commission has provided inadequate notice of its proposed rule lack merit. In fact, Huawei’s claim of vagueness,²⁹² and CCA’s assertion that the Commission has given “little indication here what a final rule might look

²⁸⁹ See, e.g., *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.* 467 U.S. 837, 42-43 (1984); *AT&T v. FCC*, 832 F.2d 1285, 1291 (D.C. Cir. 1987); *Office of Commc’n of United Church of Christ v. FCC*, 707 F.2d 1413, 1424 (D.C. Cir. 1983).

²⁹⁰ See, e.g., *Beach Commc’ns*, 508 U.S. at 316 (citing *Williamson*).

²⁹¹ *Am. Exp.-Isbrandtsen Lines, Inc. v. Fed. Mar. Com.*, 389 F.2d 962, 972 (D.C. Cir. 1968) (citing *Ry. Express Agency, Inc. v. New York*, 336 U.S. 106, 110 (1949)).

²⁹² Huawei Comments at 36.

like,”²⁹³ are difficult to take seriously. The Commission’s proposed one-sentence rule is not difficult to understand: “No universal service support may be used to purchase or obtain any equipment or services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain.” Perhaps the *only* additional element needed to put this rule into immediate and practical effect for USF recipients is a definition of the term “company posing a national security threat to the integrity of communications networks or the communications supply chain.” To that end, the Notice lays out several very specific alternatives, including language that could be converted to rule text nearly verbatim if the Commission so chooses.²⁹⁴ For APA purposes, the Commission has more than adequately met its burden.²⁹⁵

Of course, TIA has urged the Commission to provide additional clarity and focus on several points. Our suggested rule text, for example, addresses not just which companies would be covered, but also includes narrowing constructions with greater detail for the original terms “equipment” and “services,” an attestation procedure for implementation that would provide manufacturers with flexibility, and a means to address the Commission’s concern over white-

²⁹³ CCA Comments at 48 (citing *Home Box Office*, 567 F.2d at 36).

²⁹⁴ See Notice ¶ 21 (“[F]or example, we could define covered companies as those specifically barred by the National Defense Authorization Act from providing a substantial or essential component, or critical technology, of any system, to any federal agency or component thereof. Or we could define covered companies as those that the National Defense Authorization Act specifically bars from developing or providing equipment or services, of any kind listed in the NDAA, to be used, obtained, or procured by any federal agency or component thereof.”); see also *id.* ¶¶ 20, 22-23 (proposing alternative approaches).

²⁹⁵ 5 U.S.C. § 553(b)(3) (requiring notice to provide “either the terms or substance of the proposed rule or a description of the subjects and issues involved”).

labeling.²⁹⁶ Each of these elements is demonstrably a “logical outgrowth” of the Commission’s proposed rule, as they are encompassed by specific requests for comment in the Notice.²⁹⁷

The Commission therefore would be on procedurally sound grounds to adopt TIA’s suggested rule text, or any similarly well-explicated rule text, that builds on the Commission’s initial proposal in ways specifically contemplated by the Notice. CCA argues, however, that the “logical-growth doctrine has limits” and that the Commission has failed to offer any indication of what a final rule might look like, citing a 1983 D.C. Circuit case.²⁹⁸ Unlike the EPA’s rule in that case, the Commission has provided adequate notice of the possibility that it might adopt a rule that is slightly different from but comparable to the one proposed in the Notice,²⁹⁹ such as the one proposed by TIA. TIA’s proposed text does not represent a radically different approach to that found in the Notice – the initial prohibition language is mostly the same as the Notice – but simply provides greater detail and clearer limits.³⁰⁰ As CCA points out, these are the sort of modifications that the Notice expressly invited in seeking comments.³⁰¹ Based on the record in

²⁹⁶ TIA Comments at Appendix.

²⁹⁷ See, e.g., *U.S. Telecomm. Ass’n v. FCC*, 825 F.3d 674, 700 (D.C. Cir. 2016) (the logical outgrowth doctrine can be satisfied if parties “should have anticipated” a change was possible, or when a notice “expressly asked for comments on a particular issue or otherwise made clear the agency was contemplating a particular change”) (citing *CSX Transp., Inc. v. Surface Transp. Board*, 584 F.3d 1076, 1081 (D.C. Cir. 2009)); see also, e.g., Notice ¶ 15 (suggesting a components-based approach, consistent with TIA’s proposed language).

²⁹⁸ CCA Comments at 48 (citing *Small Refiner Lead Phase-Down Task Force v. EPA*, 705 F.2d 506 (D.C. Cir. 1983)).

²⁹⁹ See, e.g., Notice ¶¶ 14, 34 (seeking comment on possible modifications to the Notice’s proposed rule).

³⁰⁰ See TIA Comments at Appendix.

³⁰¹ CCA Comments at 41-43.

this proceeding, the Commission has clearly provided adequate notice of its proposal and possible variations on it.

C. A Narrowly Tailored Rule Would Be Constitutional.

Huawei (at great length) and CCA (much more briefly) argue that a narrowly tailored rule similar to that contemplated by the Notice would violate the U.S. Constitution.³⁰² These claims vastly overstate and mischaracterize the effect of the sort of rule being contemplated in this docket. The type of rule proposed by the Notice would be a prospective rule of general applicability based, *inter alia*, on determinations made by expert security agencies or Congress, which would have a limited and context-specific effect on any prohibited suppliers. To the extent due process protections are even triggered by this narrow rule, they are satisfied by this rulemaking. Further, arguments that a rule comparable to that in the Notice would constitute a regulatory taking are inaccurate, because carriers retain some economic value in their equipment and the Commission’s action to promote national security is both permissible under law and owed substantial deference. Finally, the proposed rule would not constitute a bill of attainder because it is premised on national security concerns, not punitive purposes, and the rule is related to a rational legislative purpose.

1. To the Extent It Applies, the Due Process Clause Does Not Require an Individualized Hearing Before Adoption of a Rule of General Applicability Whose Implementation Is Guided By Determinations Made by Congress or by Other Agencies.

As an initial matter, in claiming a due process violation, neither Huawei nor CCA establish any cognizable deprivation of “liberty” that must be preceded by “due process.” In order to squeeze its circumstances into applicable case law, Huawei dramatically overstates what

³⁰² Huawei Comments at 61-86; CCA Comments at 41-43.

the sort of rule at issue here would do. First, contrary to Huawei’s claim, no company will be “broadly preclude[d] ... from a chosen trade or business.”³⁰³ Instead, any prohibited supplier will remain able to conduct business with a broad array of customers.³⁰⁴ Second, and again contrary to Huawei’s account, reputational harm alone is not sufficient to make out a due process claim – rather, Huawei must show that a rule would result in some sort of stigma plus the distinct altering or extinguishing of its “legal status.”³⁰⁵ Again, and even presuming that the adoption of a USF-related restriction here would result in some sort of new stigma (beyond that already imputed via other government actions), a narrow restriction with only limited application to a company’s sales does not result in a distinct alteration (let alone extinguishment) of Huawei’s legal status. And for the same reasons, a USF-related restriction as discussed in the Notice and opening comments would not be the equivalent of a “debarment” that might otherwise trigger due process protections. Unlike the debarment cases Huawei cites, no Commission action being contemplated here would deny Huawei or any other company the “right to follow a chosen trade.”³⁰⁶

³⁰³ Huawei Comments at 62 (quoting *Trifax Corp. v. District of Columbia*, 314 F.3d 641, 644 (D.C. Cir. 2003)).

³⁰⁴ Huawei’s suggestion that the Due Process Clause protects the “free liberty to sell [one’s] wares” is incorrect. Huawei Comments at 61 (quoting *Sekhar v. United States*, 570 U.S. 729, 733 (2013)). The case Huawei cites for this proposition did not address due process issues, and the language it quotes from that decision is part of a discussion of how to define “extortion” for purposes of identifying conduct punishable under the Hobbs Act.

³⁰⁵ See, e.g., *Shrivinski v. U.S. Coast Guard*, 673 F.3d 308, 315 (4th Cir. 2012) (citing *Paul v. Davis*, 424 U.S. 693, 711 (1976)).

³⁰⁶ *Trifax*, 314 F.3d at 643.

For its part, CCA’s claim that a rule would unfairly interfere with carriers’ expectations falls flat.³⁰⁷ As discussed elsewhere, given the long history of scrutiny of these companies, no carrier could reasonably have been oblivious to the possibility that the government might limit commercial dealings with them.³⁰⁸ And to the extent any carrier can establish expectations to the contrary, measures to mitigate the impact of a rule would provide a remedy. In short, it is not clear that due process applies here in the first place. The lack of any harm to a protected liberty interest would be even clearer if the Commission adopts some form of a waiver process, as TIA has proposed.

Even if any rule adopted in this proceeding could be shown to constitute a deprivation of liberty triggering due process, Huawei has not shown that it will be denied whatever process is due. As a general matter, the determination of what due process requires is highly fact-specific, and the Supreme Court has repeatedly rejected attempts to rigidly define and circumscribe the Fifth Amendment’s protections: “due process of law has never been a term of fixed and invariable content.”³⁰⁹ In particular, “[T]he Fifth Amendment does not require a trial-type hearing in every conceivable case of government impairment of private interest.”³¹⁰ Moreover, it

³⁰⁷ CCA Comments at 41.

³⁰⁸ *See infra* section V-C-2.

³⁰⁹ *FCC v. WJR, Goodwill Station, Inc.*, 337 U.S. 265, 275 (1949) (overruling the lower court’s determination that the Fifth Amendment obligated the FCC to permit oral argument for a radio-broadcaster petitioner who opposed the grant of a permit to another broadcaster); *see also Cafeteria & Rest. Workers Union, Local 473 AFL-CIO v. McElroy*, 367 U.S. 886, 894 (1961) (“[T]he very nature of due process negates any concept of inflexible procedures universally applicable to every imaginable situation.”).

³¹⁰ *Cafeteria & Restaurant Workers Union v. McElroy*, 367 U.S. 886 (1961) (holding that the due process clause of the Fifth Amendment is not violated where a short-order cook was denied security clearance and access to the Navy cafeteria where she worked, even though she was not advised of the specific grounds for her exclusion and was never accorded a hearing or an opportunity to refute such grounds).

is axiomatic that agencies enjoy “very broad discretion [in deciding] whether to proceed by way of adjudication or rulemaking.”³¹¹ A rulemaking can be sufficient to satisfy due process requirements.³¹²

No party is deprived of all protections simply because the Commission chose the latter option. The notice-and-comment rulemaking procedures of the Administrative Procedure Act enshrine meaningful procedural rights of public notice, transparency, and participation. Indeed, the rights that Professor Hammond alleges are withheld from Huawei – an explanation of the bases for the Commission’s proposed restriction, opportunities for Huawei to respond, and a reasoned determination logically connecting the facts adduced with the choices made – are actually present here or will be once a final order is issued.³¹³ Accordingly, Huawei’s provocative invocation of “the McCarthy era” and its strained attempt to analogize itself to an “enemy combatant” are off base and irrelevant.³¹⁴ Huawei has long been on notice of the U.S. government’s security concerns, and in this proceeding, it has and continues to have ample opportunity to respond to those allegations. Its initial submission, consisting of hundreds of pages, shows that Huawei is fully capable of taking advantage of that opportunity.

³¹¹ *City of Arlington v. FCC*, 668 F.3d 229, 240 (5th Cir. 2012); *see also SEC v. Chenery Corp.*, 332 U.S. 194, 202 (1947) (“[A]n administrative agency must be equipped to act either by general rule or by individual order. To insist upon one form of action to the exclusion of the other is to exalt form over necessity.”); *id.* at 203 (“[T]he choice made between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency.”) (citing *Columbia Broadcasting System v. United States*, 316 U.S. 407, 421 (1942)).

³¹² *See, e.g., United States v. Allegheny-Ludlum Steel Corp.*, 406 U.S. 742 (1972); *United States v. Florida East Coast Ry. Co.*, 410 U.S. 224 (1973).

³¹³ Huawei Comments, Ex. H, Hammond Decl. at 6-9.

³¹⁴ *See, e.g.,* Huawei Comments at 61, 63, 67.

Furthermore, the Fifth Amendment is no shield against an otherwise valid scheme of regulation, merely because it disturbs the profitability of a few businesses.³¹⁵ This is no less true when a rulemaking of general applicability *de facto* affects only a single business. *Law Motor Freight, Inc. v. Civil Aeronautics Board*, for example, concerned a rulemaking petition that declared one city within the other city’s pickup and delivery area – a determination that burdened solely plaintiff’s motor carrier business.³¹⁶ Rejecting plaintiff’s contention that due process obligated the Civil Aeronautics Board to proceed via adjudication because the petition affected only two parties, the Court of Appeals for the First Circuit reasoned:

[T]his falls within the ambit of rule-making. ... The order is of “future effect.” It is an agency statement of both general and particular applicability. While addressed to a named applicant, it authorizes pickup and delivery services in a particular area which determination is available to all other air carriers and air freight forwarders.³¹⁷

Here, as in *Law Motor Freight, Inc.*, the agency is instituting a rulemaking to address issues of particular and general applicability: it has adduced some evidence leading it preliminarily conclude that equipment from certain suppliers pose a national security risk to the nation’s telecommunications infrastructure or supply chain networks, and it seeks to establish procedures that will enable it to identify nimbly similar threats in the future. As a result, it is distinguishable

³¹⁵ *Am. Trucking Ass’n v. United States*, 344 U.S. 298, 322-23 & n.20 (1953).

³¹⁶ 364 F.2d 139 (1st Cir. 1966).

³¹⁷ *Id.* at 143.

from those cases cited by Huawei and Hammond which solely concern the adjudication of individual rights.³¹⁸

Huawei's and CCA's further claim that they must be provided access to classified evidence is moot for the simple reason that the Commission has not relied on any such material.³¹⁹ To the extent the Commission ultimately relies on confidential information submitted pursuant to the protective order adopted in this proceeding, Huawei can review that information provided that it complies with the necessary prerequisites. And to the extent Huawei's complaint is that other government actions against it were premised on classified information that it was unable to view at the relevant time, this is the wrong forum to pursue that grievance.

2. A Narrowly Tailored Rule Would Not Constitute a Regulatory Taking.

Several commenters assert that the Commission's proposed rule would constitute a regulatory taking because it would deny some carriers of "all economically beneficial or productive use" of their property.³²⁰ These commenters argue that the proposed rule would render pre-existing equipment from prohibited suppliers useless because these carriers would be unable to upgrade, repair, or service this equipment, thus frustrating significant investment-

³¹⁸ Notably, the *Law Motor Freight* court further distinguished its facts from *Wong Yang Sung v. McGrath et al.*, 339 U.S. 33 (1950) and *Hornsby v. Allen et al.*, 326 F.2d 605 (5th Cir. 1964), cited by Huawei and Hammond. See Huawei Comments at 65 (citing *Wong Yang Sung*); Hammond Decl. at 3 n.10, 8 (citing *Wong Yang Sung*), 6 n.26 (citing *Hornsby*). The court noted that those cases involved circumstances where "the individual or company was a party ... seeking a license to operate a liquor store (*Hornsby*), or resisting deportation (*Wong Yang Sung*). All, therefore, involved a specific adjudication of basic rights, wholly *divorced from any purpose of setting agency policy for the future.*" 364 F.2d at 144 (emphasis added).

³¹⁹ CCA Comments at 42; Huawei Comments at 52, 67-68.

³²⁰ CCA Comments at 42 (citing *Lucas v. S.C. Coastal Council*, 505 U.S. 1003, 1015 (1992)); PRTC Comments at 7.

backed expectations.³²¹ According to these commenters, the Commission must provide some form of compensation to carriers whose equipment suffers a diminution of value as a result of this rule.³²²

As described in section III-D above, TIA agrees that the Commission should consider reasonable means of mitigating any burdens incurred by affected carriers. Regardless of whether the Commission elects to go down that path, however, claims that a rule such as that proposed in the Notice would constitute a regulatory taking are overstated.

As an initial matter, Commission precedent makes clear that its proposal to condition USF support would not implicate carriers' Fifth Amendment rights *at all*. In 2011, the Commission soundly rejected the argument that USF rule changes would destroy the value of existing networks and result in a regulatory taking. As the Commission explained:

Commenters seem to suggest that they are entitled to continued USF support as a matter of right. Precedent makes clear, however, that carriers have no vested property interest in USF. To recognize a property interest, carriers must "have a legitimate claim of entitlement to" USF support. Such entitlement would not be established by the Constitution, but by independent sources of law. Section 254 does not expressly or impliedly provide that particular companies are entitled to ongoing USF support. Indeed, there is no statutory provision or Commission rule that provides companies with a vested right to continued receipt of support at current levels, and we are not aware of any other, independent source of law that gives particular companies an entitlement to ongoing USF support. Carriers, therefore, have no property interest in or right to continued USF support.³²³

Even if the Commission departs from this precedent and recognizes that a vested property right exists in this situation, the Commission's proposed rule would not result in a *per se*

³²¹ CCA Comments at 42; PRTC Comments at 7.

³²² CCA Comments at 42; PRTC Comments at 7.

³²³ *Connect America R&O*, 26 FCC Rcd at 17770 ¶ 293.

regulatory taking, as commenters allege.³²⁴ As the Supreme Court has recognized, a *per se* taking can occur only in the “extraordinary” and “relatively rare” case when a regulation results in a *total* diminution in the value of the party’s affected property interest.³²⁵ Here, the Commission’s proposed rule would not come anywhere close to eliminating the value of carriers’ pre-existing equipment, because the rule would apply on a prospective basis only.³²⁶ The proposed approach would not force carriers to rip out any existing equipment but would instead allow carriers to continue using their existing equipment for the remainder of its useful life.

Moreover, even if the proposed rule impacts the useful life of pre-existing equipment by limiting a carrier’s ability to upgrade, repair, or service its equipment, this would not constitute a “partial” regulatory taking. In assessing whether such a taking has occurred, courts consider: (1) the economic impact of the regulation on the regulated party; (2) the extent to which the regulation interferes with the regulated party’s reasonable investment-backed expectations; and (3) the “character” of the government action.³²⁷ The carriers cannot establish a partial regulatory taking under this test.

First, as described above, carriers would likely be able to continue using equipment that they have previously purchased from prohibited companies under the proposed rule. Thus, the

³²⁴ CCA Comments at 42; PRTC Comments at 7.

³²⁵ *Lucas*, 505 U.S. at 1017-18; *see also id.* at 1019 (“We think ... that when the owner of real property has been called upon to sacrifice *all* economically beneficial uses in the name of the common good ... he has suffered a taking.”).

³²⁶ Notice ¶ 17.

³²⁷ *Penn Cent. Transp. Co. v. New York City*, 438 U.S. 104, 124 (1978).

degree of diminution in the market value of said equipment would not be severe.³²⁸ Moreover, as described in section III-B above, estimates by carriers of the costs that would be imposed on them by the new rule are likely overstated.

Second, the proposed rule would not interfere with carriers' reasonable investment-backed expectations.³²⁹ As the Supreme Court has observed, under this factor “[t]hose who do business in the regulated field cannot object if the legislative scheme is buttressed by subsequent amendments to achieve the legislative end.”³³⁰ Furthermore, since the release of the high-profile 2012 HPSCI report – and possibly earlier – every carrier in the United States has either known, or reasonably should have known, that products from companies such as Huawei and ZTE were viewed as creating significant security concerns for communications networks.³³¹ Given all of the subsequent federal government actions taken against these two companies in the years since, it is difficult to imagine that any carrier investing in equipment from them was unaware of the possibility that the U.S. government might take action to restrict such products. Indeed, *one of CCA's declarants* explicitly acknowledges that his company intentionally avoided Huawei

³²⁸ In this regard, the Supreme Court has said that “mere diminution in the value of property, however serious,” cannot by itself establish a taking, citing cases in which value diminutions of 75 percent and 92.5 percent were upheld. *Concrete Pipe & Prods. of Cal., Inc. v. Constr. Laborers Pension Trust*, 508 U.S. 602, 645 (1993).

³²⁹ *Lucas*, 505 U.S. at 1034 (“[T]he test must be whether the deprivation is contrary to *reasonable*, investment-backed expectations.”) (emphasis added).

³³⁰ *Connolly v. Pension Benefit Guar. Corp.*, 475 U.S. 211, 227 (1986) (quoting *FHA v. The Darlington, Inc.*, 358 U.S. 84, 91 (1958)).

³³¹ Notice ¶¶ 3-6; HPSCI Report at iv.

products to protect the security of its networks, demonstrating that at least some smaller providers were acutely aware of these concerns.³³²

Third, with respect to the “character” of the government action, this is not a case where the Commission would be physically invading or permanently appropriating carriers’ property for its own use. Instead, any government interference would arise “from a public program that adjusts the benefits and burdens of economic life to promote the public good,” and Supreme Court precedent makes clear that this “does not constitute a taking requiring Government compensation.”³³³ Finally, TIA notes that courts are particularly reluctant to find a Takings Clause violation in the context of national security.³³⁴ This heightened judicial deference extends beyond national security threats of the “traditional-war variety”³³⁵ to situations involving foreign property or a contract with a foreign company.³³⁶ As a result, any company that claims that it is being harmed by the Commission’s rule would face an even higher bar under takings jurisprudence.

³³² CCA Comments, DiRico Decl. ¶ 3 (“Viaero has consciously used a US-based vendor separate and distinct from Huawei for our firewalls, routers and switches. ... This gives Viaero protection from any malicious act by Huawei or anybody else.”).

³³³ *Connolly*, 475 U.S. at 225.

³³⁴ See Robert Meltz, *Federal Responses to International Conflict and Terrorism: Property Rights Issues*, Cong. Research Serv., RL32629, at 2, Oct. 6, 2004, <https://fas.org/sgp/crs/terror/RL32629.pdf> (“International dangers have consistently prompted courts to extend deference to responsive government measures when dealing with regulatory takings claims.”).

³³⁵ *Id.* at 3.

³³⁶ *Id.* at 13 (citing *Chang v. United States*, 859 F.2d 893 (Fed. Cir. 1988); *767 Third Avenue Assocs. v. United States*, 48 F.3d 1575 (Fed. Cir. 1995); *Paradissiotis v. United States*, 304 F.3d 1271 (Fed. Cir. 2002)).

3. The Rule Would Not Be a Bill of Attainder.

Huawei argues that the Commission’s proposed rule would violate the Bill of Attainder Clause because it would create a “blacklist” of companies barred from selling their products to USF recipients.³³⁷ A law or agency regulation constitutes a bill of attainder “if it (1) applies with specificity, and (2) imposes punishment.”³³⁸ By its very nature, a rule similar to that contemplated by the Notice may need to apply some level of specificity to achieve the goal of protecting the security of the U.S. telecommunications network from entities that have been determined to pose a threat to national security. Contrary to Huawei’s assertion, however, this would not mean that the proposed rule would impose a forbidden “punishment.”

The recent opinion by the federal district court in *Kaspersky Lab, Inc. v. U.S. Dep’t of Homeland Security*,³³⁹ which upheld a congressional ban on the federal government procuring software, equipment, and services from Kaspersky Lab based on national security concerns, is instructive on this point. In that case, Kaspersky Lab made an argument similar to the position that Huawei is staking out in this proceeding. Specifically, Kaspersky Lab argued that the punitive nature of the legislation at issue was “demonstrated by the fact that it singles out Kaspersky Lab and no other cybersecurity vendors.”³⁴⁰ The court rejected this argument. While the court acknowledged that the specificity of a law is “one factor” that a court may consider when determining whether a law is punitive,³⁴¹ it emphasized that “specificity alone is not

³³⁷ Huawei Comments at 78-80.

³³⁸ *Foretich v. United States*, 351 F.3d 1198, 1217 (D.C. Cir. 2003) (quoting *BellSouth Corp. v. FCC*, 162 F.3d 678, 683 (D.C. Cir. 1998)).

³³⁹ 2018 U.S. Dist. LEXIS 89510 (D.D.C. May 30, 2018) (“*Kaspersky*”).

³⁴⁰ *Id.* at *55.

³⁴¹ *Id.*

sufficient to establish that a law has a punitive function.”³⁴² The court then went on to explain that “[w]here a law targets a particular individual (or corporation) because there is a legitimate nonpunitive reason to take such targeted action, specificity is not improper and does not evince punishment.”³⁴³

Here, too, there can be no doubt that the Commission has a legitimate, non-punitive reason to take targeted action in the USF context. The Notice details actions already taken by Congress and members of the Executive Branch as evidence that products sold by companies that would be prohibited from the USF market create vulnerabilities in U.S. communications networks and present unique threats to U.S. national security.³⁴⁴ A rule removing these potential threats would not be a “bill of attainder,” but a rational approach to effectuate a legitimate public purpose.

CONCLUSION

As TIA explained in our initial comments, the Commission faces a truly extraordinary situation. National security concerns regarding certain suppliers of communications products have led to a wide variety of actions at home and abroad. Even so, the basic circumstances remain the same. The Commission has an important but limited role to play. Its actions will set an example for other federal agencies, advance the discussion among policymakers in Congress and the Administration, and potentially guide the actions of other telecom regulators around the world. The Commission should establish a narrowly tailored rule that focuses on the problems at hand, while also keeping an eye on the future.

³⁴² *Id.* at *56 (citing *Nixon v. Adm’r of Gen. Servs.*, 433 U.S. 425, 470-71 (1977); *ACORN v. United States*, 618 F.3d 125, 138-39 (2d Cir. 2010)).

³⁴³ *Id.* (citing *Nixon*, 433 U.S. at 472).

³⁴⁴ *See* Notice ¶¶ 3-11.

Since the opening comments were filed, TIA has continued to engage in active discussions with and among our member companies: the manufacturers and suppliers of the world's ICT products. We have also continued to work with Congress and other stakeholders seeking to address these problems across the government. We look forward to working with the Commission as the agency considers its next steps on these very important issues in the months ahead.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY
ASSOCIATION

By: /s/ Cinnamon Rogers

Cinnamon Rogers
Senior Vice President, Government Affairs

Dileep Srihari
Senior Policy Counsel and Director, Gov't Affairs

K.C. Swanson
Director, Global Policy

Savannah Schaefer
Policy Counsel, Government Affairs

Colin Black Andrews
Policy Counsel, Government Affairs

TELECOMMUNICATIONS INDUSTRY
ASSOCIATION
1320 N. Courthouse Road
Suite 200
Arlington, VA 22201
(703) 907-7700

July 2, 2018

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

DECLARATION OF CINNAMON ROGERS

I, Cinnamon Rogers, declare as follows:

1. My name is Cinnamon Rogers. I am over the age of 18 and competent to make this declaration. The statements in this declaration are true and within my personal knowledge.
2. I am the Senior Vice President of Government Affairs for the Telecommunications Industry Association (“TIA”). TIA is the leading trade association for the manufacturers, suppliers, service enablers, distributors, and system integrators of information and communications technology (“ICT”) products, with a membership of more than 260 companies.
3. I communicate regularly with TIA members about policy and legal developments that may affect the telecommunications market generally or their businesses directly. I work closely with my staff, which includes individuals with expertise in government relations, regulatory affairs, and legal policy, to communicate our members’ concerns and opinions to appropriate agencies, committees, legislators, and staff in Washington, D.C., and across the country. My staff is also in daily contact with our members on issues of vital importance to the business and regulatory environment affecting ICT equipment manufacturers and suppliers.

Carriers Using Huawei or ZTE Equipment

4. TIA is not aware of any publicly-available data regarding the number of carriers that use Huawei or ZTE equipment in their infrastructure.

5. TIA member companies have obtained information, and accordingly maintain proprietary data, regarding which wireless carriers in the United States are currently believed to use Huawei or ZTE equipment. This data has been obtained and is maintained for market intelligence purposes. At TIA's request, relevant portions of this data have recently been shared with me and/or my staff for the sole purpose of engaging in policy advocacy in this proceeding. Information on use of Huawei and ZTE equipment by wireline service providers has not been made available to TIA.

6. The data shared with TIA indicates that there are currently 13 U.S. wireless carriers, all of which are small and/or rural carriers and all of which receive USF support, that use either Huawei (11) or ZTE (2) equipment as a substantial part of their network infrastructure. I and/or my staff have been further informed as follows:

a. Nine of these deployments are mobile wireless access while the other four are predominantly fixed wireless deployments.

b. The mobile wireless deployments represent approximately 1,300 cell sites in total, and all of the deployments including primarily fixed wireless deployments represent less than 1,500 sites in total.

c. There are approximately 300,000 cell sites in the United States, and Huawei and ZTE's share of the U.S. wireless infrastructure market therefore appears to be approximately one half of one percent or less.

7. There is good reason to believe that the data shared with TIA reflects a reasonably complete picture of the use of Huawei and ZTE equipment by U.S. wireless carriers. Notably, the list of 13 carriers includes all seven of the carriers that filed declarations attached to the initial comments of the Competitive Carriers Association (“CCA”) in this proceeding:


- a. SI Wireless LCC d/b/a MobileNation
- b. NE Colorado Cellular d/b/a Viaero Wireless
- c. James Valley Telecommunications
- d. United Telephone Association, Inc.
- e. Nemont Telephone Cooperative, Inc. / Sagebrush Cellular, Inc.
- f. Pine Belt Cellular, Inc.
- g. Union Telephone Company d/b/a Union Wireless¹

8. At TIA’s request for the sole purpose of engaging in policy advocacy in this proceeding, I and/or my staff have been informed that an equipment price of \$100,000 per cell site, not counting installation costs, would be a reasonable upper cost limit for current-generation macrocell LTE equipment in the United States market. Assuming that the per-site costs for fixed wireless equipment (200 sites) are roughly comparable to those for cell sites, and based on the information above regarding number of cell sites, a reasonable upper bound for the total cost of replacement equipment for all 13 affected wireless carriers would therefore be on the order of 1,500 sites x \$100,000 per site = \$150 million. However, depending upon specific circumstances and commercial arrangements, the equipment cost for any given customer would likely be significantly lower than \$100,000-per-site.

¹ See Comments of Competitive Carriers Association, filed June 1, 2018 in WC Docket No. 18-89, at Appendix.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed on: 6/29/18
(date)



Cinnamon Rogers