Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Huawei Designation	)	PS Docket No. 19-351
	)	
ZTE Designation	)	PS Docket No. 19-352
	)	

Comments of
WTA – Advocates for Rural Broadband

WTA – Advocates for Rural Broadband[1] ("WTA") files these comments in response to the Public Notice,[2] released by the Public Safety and Homeland Security Bureau on March 13, 2020, seeking comment on the applicability of provisions in the Secure Networks Act [3] ("Act") to the Commission's designations of Huawei and ZTE as covered companies in its *Protecting Against National Security Threats* Report and Order.[4]

Throughout this proceeding, WTA has represented the interests of its rural local exchange carrier ("RLEC") membership. While WTA primarily represents the wireline interests of its members, a limited number have mobile wireless offerings and have Huawei and ZTE equipment in their networks. Any potential action will undoubtedly interrupt their normal business operations. As such, WTA has advocated for policies that will minimize any service

[1] *WTA - Advocates for Rural Broadband* is a national trade association that represents more than 340 rural telecommunications providers offering voice, broadband, and video-related services in rural America. Its members serve some of the most rural and hard-to-serve communities in the country and are providers of last resort to those communities.
[2] Public Notice*,* PS Docket Nos. 19-351, 19-352, released March 13, 2020.
[3] See Pub. L. 116-124, 133 Stat. 158 (2020), ("Act").
[4] Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, et al., Report and Order, Further Notice of Proposed Rulemaking, Order, WC Docket Nos. 18-89, et al., (2019).

disruptions to its affected members and their customers. This, among other things, has included protecting the sufficiency of the Universal Service Fund for all eligible telecommunications carriers (not just those with covered equipment in their networks) and ensuring that any "rip and replace" program is designed to maintain, and when possible, improve existing network coverage.

WTA did not file comments in the designation proceedings of Huawei and ZTE. However, it is very interested in how the Commission interprets the Act in these proceedings as well as in the *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs* proceeding (WC Docket No. 18-89).

A plain reading of the Act requires the Commission to replace its current designation process with an equipment-centric approach instead of the company-centric approach it adopted in its Report and Order. Under the Act, the Commission must now determine if individual pieces of equipment and services pose a security risk rather than deeming all equipment from a provider to be a risk.

Provisions in the Secure Networks Act Preempt the Commission from Using the Designation Process Previously Adopted in the Report and Order

Going forward, the Commission must reconcile the fact that the Act passed by Congress significantly alters the designation process it previously adopted. Notably, rather than focusing on the company as a whole, the Act focuses on determining whether specific equipment produced by a company poses a national security threat. It also provides the Commission with specific criterion to use in determining if a company poses a national security threat – giving the Commission less discretion.

In its Report and Order, the Commission placed a blanket ban on all equipment from covered companies that pose a national security threat and rejected calls from commenters to identify specific equipment that poses a national security threat. Instead, the Commission reasoned that such a broad prohibition was the only reliable protection against the "wide-ranging nature of the potential threats to our networks."[5] The Commission also stated that it would be the most efficient course of action since it would give providers clear certainty as to what equipment is acceptable to use.[6]

The Act does not enact such a broad prohibition on a company as a whole, but rather speaks specifically about certain equipment. The Act instructs the Commission to establish a list of covered equipment using a two-part test. First, the Commission must place equipment on this list "*if and only if*" it determines the equipment is produced by an entity that poses an unacceptable risk to the national security of the United States based on four determinations:

(1) A specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1322(a) of title 41, United States Code.
(2) A specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain).
(3) The communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 1918).
(4) A specific determination made by an appropriate national security agency.

This is a departure from the Report and Order where the Commission gave itself discretion in designating companies as covered, stating that it would "use all available evidence to determine

[5] Report and Order at ¶ 67-68.
[6] Id. at ¶ 69.

whether an entity poses a national security threat."[7] Now, the Commission must rely on a prescribed set of sources when deciding if an entity is a threat.

Second, the Commission must find that the equipment is capable of:

> (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles;
> (B) causing the network of a provider of advanced communications service to be disrupted remotely; or
> (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.[8]

Therefore, in order for the equipment to be designated as covered, it must be produced by a company deemed to be a security risk and the equipment in question must be able to route/redirect traffic or grant visibility into a network, disrupt a network, or otherwise be a risk to national security. This is a new requirement that the Report and Order did not consider as it only deemed equipment as covered based upon the company that produced it.

A plain reading of the statute requires the Commission to now adopt a more thorough review of specific equipment. Congress included such language in Section 2(b)(2) because it understood that not all parts of a network are equal when it comes to being a security risk. A company that is a security risk may very well produce equipment that does not pose a risk. For example, while equipment inside the core of a network may be capable of granting visibility into or disrupting a network, equipment on the edge of a network is potentially and likely unable to. If the Commission moves forward with a rip and replace program, removing only the equipment that actually poses a security risk (at least initially) would save taxpayer dollars as well as help to

[7] Report and Order at ¶ 41. "Examples of such evidence may include, but are not limited to: determinations by the Commission, Congress or the President that an entity poses a national security threat; determinations by other executive agencies that an entity poses a national security threat; and, any other available evidence, whether open source or classified, that an entity poses a national security threat."
[8] The Act at Section 2(b)(2).

ensure there is enough funding to remove all equipment that poses a risk. Meanwhile, if the Commission deems certain equipment to not be a security risk despite it being produced by a covered entity, it would minimize the disruption to carriers who would no longer have to rip and replace such equipment. In this instance, the network equipment least likely to pose a security risk is on the edge of the network, but is the most expensive and time-consuming to replace due to the likely necessity of hiring tower crews to service hard-to-reach areas. Therefore, moving forward, the Commission must create a list of covered equipment by providing a thorough analysis of individual pieces of equipment and then explain how that equipment is able to route/redirect traffic or grant visibility into a network, disrupt a network, or otherwise be a risk to national security.

Further, the Commission must also discontinue the designation process it adopted in its Report and Order. Congress has now spoken on the issue of supply chain and the question of how to handle equipment that may pose a national security threat. It has given the Commission explicit direction to create a list of equipment and services that pose a security risk using specific sources determined by Congress. In adopting its previous Report and Order, the Commission acted with implicit authority delegated to it under Section 254. This interpretation of Section 254 is now at odds with clear guidance from Congress, and it is no longer eligible for Chevron deference.[9]

[9] Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837 (1984).

Conclusion

In the Act, Congress directed the Commission to establish a list of specific equipment that poses a security threat. This is opposite to the designation process the Commission established in its recent Report and Order that focused on designating an entire company a security threat. The Commission must discontinue the designation process it adopted and replace it with the new process outlined by Congress that calls for creating a list of equipment that poses a threat.

Respectfully submitted,

WTA – Advocates for Rural Broadband

By: /s/ Derrick B. Owens
Derrick B. Owens
Senior Vice President of Government & Industry Affairs
400 Seventh Street, NW, Suite 406
Washington, DC 20004
(202) 548-0202

By: /s/ Bill Durdach
Bill Durdach
Director of Government Affairs
400 Seventh Street, NW, Suite 406
Washington, DC 20004
(202) 548-0202

By: /s/ Gerard J. Duffy
Gerard J. Duffy
Regulatory Counsel
Blooston, Mordkofsky, Dickens, Duffy & Prendergast, LLP
2120 L Street NW, Suite 300
Washington, DC 20037
(202) 659-0830

March 27, 2020