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

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

Comments of
WTA – Advocates for Rural Broadband

WTA – Advocates for Rural Broadband[1] files these comments in response to the proposals in the Commission's Notice of Proposed Rulemaking ("NPRM"),[2] adopted on April 17, 2018, to prohibit Universal Service Fund ("USF") dollars from being spent in the future on equipment, software, and services from companies that pose a national security threat to the United States.

WTA's members are rural local exchange carriers ("RLECs"), and they rely on USF support to help build and maintain communications networks in high cost rural areas. They have lengthy and significant experience in constructing networks that are designed to bridge the digital divide. They are providers of last resort to their communities and are dedicated to providing quality voice and broadband services to all

[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] *In re Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Notice of Proposed Rulemaking, released April 18, 2018 ("NPRM"), available at https://www.fcc.gov/document/fcc-proposes-protect-national-security-through-fcc-programs-0.

residents of their rural service areas that are reasonably comparable in quality and price to those available in urban areas. A major feature of these diverse rural areas are the much longer than average distances that must be traversed to serve customers and the high costs associated with doing so. As a result, this makes it extremely difficult to deploy networks in a manner similar to how urban providers would. Therefore, as responsible recipients of USF funds, WTA members make sure that money is used efficiently and wisely. WTA members are especially sensitive to cost, and therefore, rely on the global supply chain, which gives them a greater choice of products, and at price points that are affordable, when deploying their networks.

In this filing, WTA wishes to outline the limited extent to which its members are reliant on products from companies that may pose a national security threat and requests that any future Commission policy be prospective only and clearly specify the equipment, software, and services that USF recipients must not use when constructing networks.

Like the Commission, WTA recognizes the cybersecurity risks networks face and the critical need to make sure that our nation's communications networks cannot be compromised or harmed by its enemies. As a representative of purchasers of telecommunications equipment, WTA hopes that all foreign vendors will be convinced to become transparent and to work with the U.S. Government to ensure that their products do not pose a threat to national security. WTA believes that inspection and compliance processes can be developed and implemented that will resolve national security concerns before equipment software and services are purchased and installed. Such a solution can protect our national security while avoiding prohibitions and costs that make it even

harder and more expensive to serve those that live in the most difficult to reach parts of our country.

SOME WTA MEMBERS THAT ALSO OFFER MOBILE WIRELESS SERVICE USE EQUIPMENT POTENTIALLY IMPACTED BY A BAN

WTA members are community-based telecommunications providers in the hardest to serve areas in the country. All WTA members are traditional wireline voice service providers that have evolved over the years to become broadband service providers. Some WTA members offer or resell mobile wireless voice service as well.

When the NPRM was first released, WTA conducted outreach and polled its membership to learn to what extent members used products from ZTE, Huawei, or Kaspersky Lab.[3] No responding WTA members that offer only wireline service stated that they used any technology from those three companies. However, a few WTA members that offer mobile wireless voice service indicated they use equipment from one of those companies, specifically Huawei. Those members who are using Huawei products cited cost, customer service, and reliability as reasons for choosing to procure equipment from the company.[4]

---

[3] On May 25, 2018, the White House announced a deal between the Commerce Department and ZTE that would end a ban that barred ZTE from purchasing components from the United States, which effectively shuttered the company. David Shepardson and Karen Freifeld, U.S. reaches deal to keep China's ZTE in business: congressional aide, Reuters, May 25, 2018, available at https://www.reuters.com/article/us-usa-trade-china-zte/u-s-reaches-deal-to-keep-chinas-zte-in-business-congressional-aide-idUSKCN1IQ2JY.

[4] WTA notes that positive statements made in regard to potentially covered companies are based on member company experiences and should not be as seen as undermining any of the serious issues raised in the NPRM. The security of our nation's networks is paramount.

Specifically, one member stated that when choosing vendors for their recent 4G deployment it considered several other well-known vendors that sell globally. However, the member noted those vendors were simply unaffordable at two to four times the cost of using Huawei. The member also noted that one prominent alternative vendor did not even give it a price quote for the deployment only stating that a small company "would be unable to afford them." The WTA member company moved forward with Huawei and has been using Huawei equipment throughout its 4G deployment. The company has spent more than $25 million on Huawei equipment for its wireless network except for its participation in the Verizon Wireless LTE in Rural America program and its fixed wireless networks. The company stated that because of its business plan, it expects to continue using the equipment from the Huawei deployment for five to seven years and that it has a maintenance agreement with Huawei through 2021. The company stated that it goes to great lengths to test the equipment for security issues and has never encountered an issue that it is aware of that has threatened the security of its customers or the nation. The company added that Huawei's equipment is efficient and works very well for the company's purposes, especially at the reduced cost. The WTA member also indicated that Huawei's customer service has been exceptional and that Huawei representatives are readily available to address any issues that need resolving with its products.

Another WTA member chose Huawei four years ago when another vendor fell behind on a critical network upgrade, and the member added that Huawei put an emphasis on getting the problem fixed before worrying about getting paid. The member added "Huawei has treated us better than anybody." The member also lamented about the

lack of competition in the market noting that four years ago, there were five suppliers, but today there are only two.[5]

For the WTA members that use Huawei, it appears their experiences have been positive. They say the equipment has performed as advertised and the cost of procuring the equipment and software has been more affordable than those of competitors. They also value its customer service and affordability.

THE COMMISSION SHOULD CONSIDER ALTERNATIVES BEFORE ADOPTING AN OUTRIGHT BAN ON FUNDING CERTAIN EQUIPMENT

Whereas the Huawei and ZTE equipment currently at the forefront of national security concerns has been purchased and installed to date, predominately in mobile wireless networks, WTA is concerned that similar issues may arise in the future with respect to routers and other equipment employed in fixed broadband networks.

For example, WTA is concerned that its members may be restricted or banned in the future from using equipment from a company that is not even mentioned in the NPRM or currently suspected of being a national security threat. Today's telecommunications marketplace is extremely reliant on the global supply chain where almost all telecommunications equipment can be traced to foreign countries, especially China.[6] This is especially true when components from several companies are assembled

[5] Stu Woo, Dan Strumpf, & Betsy Morris, Huawei, Seen as Possible Spy Threat, Boomed Despite U.S. Warnings, Wall Street Journal, Jan. 8, 2018, available at https://www.wsj.com/articles/huawei-long-seen-as-spy-threat-rolled-over-u-s-road-bumps-1515453829.

[6] Testimony of Dr. Charles Clancy before the House Energy and Commerce Committee, Subcommittee on Communications and Technology, Hearing on Telecommunications, Global Competitiveness, and National Security, May 16, 2018, available at

together to make one product. WTA fears that an issue with a single component could force their members to lose ongoing USF support for an entire piece of equipment.

The Commission has proposed that any ban be prospective in nature. If the Commission moves forward, it should only affect future agreements to purchase new equipment. All prior existing agreements, including agreements for maintenance and customer service, between an applicable vendor and a provider should be grandfathered. Though equipment may have already been purchased and installed, funding is still necessary to maintain and upgrade the equipment through its normal lifespan. As such, new agreements to service existing equipment should be allowed. In the past, providers made an informed decision on what equipment they should use and chose the alternative that best served their situation. Providers should not be punished retroactively for using equipment that they previously selected in a reasonable and prudent manner. Further, USF funds should continue to be used to support infrastructure that is already partially in use or currently in the process of being deployed.[7] Especially in rural areas, networks are constructed generally via a multi-year process where it is possible that one phase of a deployment will be completed a few years before other parts of a service territory are completed. Forcing a provider to abandon a portion still under construction would be inefficient and a waste of resources. [8]

---

https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-Wstate-ClancyC-20180516-U11.pdf.

[7] WTA is encouraged that the Commission has not proposed the immediate removal of applicable equipment. This would result in duplicative costs and would undoubtedly disrupt service, especially since most companies are satisfied with their current networks, as previously mentioned.

[8] Since it is a matter of national security, if the Commission finds that a ban is necessary, the Commission should provide additional funding to incentivize providers to voluntarily replace the applicable equipment.

Also, as an alternative or pre-condition to an outright ban, the Commission, in conjunction with other agencies under the Department of Commerce, should consider developing an equipment testing regime that is similar to one established in the United Kingdom.[9] Currently, in the United Kingdom, Huawei financially supports a testing center where 30 people with UK security clearances disassemble and test all Huawei equipment and software for security vulnerabilities. Though Huawei funds the testing center, the work is overseen by a board composed of mostly senior British intelligence and government officials along with three Huawei representatives.[10] Similarly, the United States (perhaps lead by the National Institute for Science and Technology and the Commission's Office of Engineering and Technology) could establish a lab to make sure equipment does not have vulnerabilities and is safe to be used in rural networks. The United States could even strengthen that model by limiting or removing any possible influence that a private company could have on the research. This would ensure the legitimacy of the lab's findings and would also offer a chance at preserving the limited competition that exists in the rural wireless marketplace.

WTA agrees with recent congressional testimony that "any further requirements or prohibitions be derived directly from broader interagency policy processes or statutory requirements."[11] As such, WTA supports dialogue between the industry and government

---

[9] Stu Woo & Dan Strumpf, All but Banned in the U.S., Chinese Giant Huawei Is Welcomed in Britain, Wall Street Journal, Feb. 23, 2018, available at https://www.wsj.com/articles/huaweis-u-k-relationship-raises-u-s-concerns-1519416947.

[10] Id.

[11] Testimony of Mr. Clete Johnson before the House Energy and Commerce Committee, Subcommittee on Communications and Technology, Hearing on Telecommunications, Global Competitiveness, and National Security, May 16, 2018, available at https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-Wstate-JohnsonC-20180516-U31.pdf.

agencies to decide which companies or equipment may be banned in the future. WTA members are concerned that rural providers will not be engaged in the decision-making process, which will result in government action being additionally burdensome for stakeholders.[12] WTA believes for a policy to be as effective as possible that substantial input must be collected from the industry, the Commission, and other agencies such as the Rural Utilities Service, with which WTA members regularly collaborate. WTA suggests that any decision to ban equipment must be communicated to the industry in an efficient and understandable manner. One possible method would be to publish a list of equipment and manufacturers that a rural provider cannot use in deployments on the Commission's and the Universal Service Administrative Company's websites. This list should be prominently displayed on the websites so carriers can easily find the information. The list should also be updated regularly to ensure that all information is timely and can be relied upon by rural providers.

CONCLUSION

WTA and its members take national security and cybersecurity very seriously and also value competition in the marketplace. Most of all, WTA and its members value certainty. As such, WTA recommends that any Commission action with respect to national security restrictions or prohibitions with respect to certain equipment and vendors should be prospective only, done with caution, and entail collaboration with affected stakeholders to the extent possible.

[12] WTA members and others serving rural America have decades of experience constructing networks in conditions unique from urban areas. Their input on a range of matters, including network efficiency and pricing, would be a valuable resource to the government as it crafts policy.

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

June 1, 2018