Published on *The National Law Review* https://natlawreview.com

Current "Whole of Government" Approach to Perceived National Security Risks from Chinese Technology Reflected in the FCC's Latest Universal Service Fund Order

Article By:

Laura H. Phillips

Nate Bolin

Qiusi Y. Newcom

On November 26, 2019, the Federal Communications Commission (FCC) voted unanimously to ban Huawei Technologies Company and ZTE Corporation equipment and services from all projects subsidized by funding from the FCC's Universal Service Fund (USF). The ban will become effective once the FCC's latest Order is published in the Federal Register.

The USF is an FCCfund that, among other things, provides subsidies to defray some of the costs of providing telecommunications services and broadband connections to geographic areas in the United States where the costs of service are high due to the relative lack of density of the population, typically rural areas. Eligible high cost carriers obtain funding so that there is rural broadband and telecommunications available at a cost that is somewhat comparable to that in non-high cost areas. Many rural wireless and other carriers, especially those receiving USF subsidy, operate on a razor-thin profit margins and had in the past turned to Huawei and ZTE equipment and services because of their lower price and network customization offerings. Those options are no longer on the table.

In an effort to "ensure that the … [USF] … [is] not used in a way that undermines or poses a threat to [the United States'] national security," the FCC designated two Chinese entities, Huawei Technologies Company and ZTE Corporation, as prohibited entities in its USF programs. Once the order becomes effective, USF recipients may no longer use monies from the USF to "purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services provided or manufactured" by these entities. USF recipients or future applicants are also required to demonstrate, as a condition of receiving future funding, that these funds are and will not be used for the covered equipment or services.

This FCC action reflects a "whole of government" approach to perceived national security threats from Chinese telecommunications and information technology companies. Other manifestations of this approach can be seen in the Section 301 investigation of Chinese technology transfer and IP policies, the Executive Order on Securing the Information and Communications Technology and

Services Supply Chain, the recently enacted Section 889 of the National Defense Authorization Act for Fiscal Year 2019, ongoing criminal and civil prosecutions, and designations of certain Chinese telecom and IT companies on various U.S. government denied party lists.

In recent months, the U.S. government's characterization of the risks posed by these companies has grown increasingly blunt. For example, in a letter filed with the FCC, Attorney General William Barr strongly endorsed the FCC's proposed restrictions on Huawei and ZTE, stating that those companies' "own track record, as well as the practices of the Chinese government, demonstrate that Huawei and ZTE cannot be trusted."

A key issue in the latest FCC action is the extent to which wireless and other carriers will have to remove and replace existing equipment and services provided or manufactured by Huawei and ZTE. While the FCC's own report on supply chain security cited that Huawei and ZTE equipment only represents "a small percentage of equipment in U.S. networks – likely in the low single digits," some industry associations pointed out that in rural markets that are most "restricted in their financial operations," Huawei and ZTE equipment and services have been a much more significant component in the wireline and wireless networks. For example, the Rural Wireless Association (RWA) has warned that if the FCC's prohibition goes into effect, more than 25% of its rural wireless carrier members will be forced to spend millions in direct costs to rip-and-replace existing equipment.

The FCC has rejected these arguments, in part out of a concern that any type of exemption now would only increase the risks from such an installed base going forward, particularly as 5G infrastructure investments are being made. Noting that most rural carriers initially chose Huawei and ZTE equipment due to their low cost, the FCC reasoned that "those low costs are likely due to favorable subsidies and other benefits bestowed by governments that are in an adversarial position to the United States." As a result, "[r]estricting the prohibition we adopt today . . . would not only undercut the purpose behind this proscription, but could actively increase the risks posed by existing equipment."

Accordingly, under the FCC's latest action, USF recipients will be prohibited from using USF monies for "upgrading the covered equipment, installing software updates on such equipment, or paying for a maintenance contract for the covered equipment." USF recipients and future applicants are additionally expected to conduct security provider security compliance audits and program integrity assurances processes and certify, at the time of applying for additional funding, to their supply chain's overall compliance. Existing USF participants, including those under multi-year "evergreen" contracts, must also expeditiously request service substitution to prevent the use of additional funding on previously approved equipment or services provided or manufactured by Huawei or ZTE.

Notably, the emphasis of this prohibition is on "using USF monies," because the FCC is "not restricting USF recipients from performing needed upgrades or maintenance to equipment procured from a covered company so long as they do not use USF funds to do so." As such, "USF recipients may continue to use equipment or services provided or produced by [Huawei and ZTE] obtained prior to" November 26, 2019. And they "remain free to seek a waiver of this prohibition in the exceptional case where they would be unable to operate their networks absent the use of USF funds to maintain or otherwise support equipment or services produced or provided by" Huawei and ZTE.

Despite this clarification, USF applicants and recipients will likely be hard-pressed to assess and address Huawei and ZTE equipment already in their supply chain, at least in the near term. Risks of losing USF funding increase when it may be difficult to discern Huawei's or ZTE's presence in a complex supply chain structure. An example is the practice of "white labeling," "where a covered

company provides equipment or services to a third-party entity for sale under that third party's brand and the purchaser may not know the covered company's equipment is part of the purchased product." The cost of conducting comprehensive supply chain audit is also not likely to be attractive to providers in rural markets that are most "restricted in their financial operations."

As the FCC's action reflects, the U.S. government's coordinated crack-down on Chinese origin telecommunications and information technology is expanding and will be with us for months, if not years, to come. Companies and investors in telecommunications networks and information technology, even those that do not qualify for or seek USF subsidy, should closely examine the latest FCC action and its potential effects on their own operations. Failure to do so could result in significant, sudden, and unexpected costs and network or product downtime.

National Law Review, Volume IX, Number 339