

Media Contact:

Tina Pelkey, (202) 418-0536

Tina.Pelkey@fcc.gov

For Immediate Release

**CHAIRMAN PAI INTRODUCES NEW RULES
TO PROTECT U.S. COMMUNICATIONS NETWORKS
FROM NATIONAL SECURITY THREATS**

New Rules Would Prohibit Recipients of FCC's Universal Service Funds from Using USF Money to Purchase Equipment or Services from Companies that Threaten National Security

WASHINGTON, October 28, 2019—Federal Communications Commission Chairman Ajit Pai today presented his colleagues with a two-part proposal that would help safeguard the nation's communications networks. The Commission will vote on this proposal at its November 19 meeting.

First, a draft Report and Order would bar communications companies from using any support they receive from the FCC's Universal Service Fund to purchase equipment or services from companies posing a national security threat, like the Chinese companies Huawei Technologies Co. and ZTE Corp. The draft Order would also establish a process for designating other suppliers that pose a national security threat.

Second, a draft Further Notice of Proposed Rulemaking would propose requiring certain carriers receiving USF funds, known as eligible telecommunications carriers, to remove existing equipment and services from designated companies from their networks, and seek comment on how to provide financial assistance to these carriers to help them transition to more trusted suppliers. The draft item would also adopt an information collection to help assess the extent to which eligible telecommunications carriers have deployed Huawei and ZTE equipment in their networks as well as the costs to remove and replace it.

Chairman Pai issued the following statement:

“When it comes to 5G and America's security, we can't afford to take a risk and hope for the best. We need to make sure our networks won't harm our national security, threaten our economic security, or undermine our values. The Chinese government has shown repeatedly that it is willing to go to extraordinary lengths to do just that. And Chinese law requires all companies subject to its jurisdiction to secretly comply with demands from Chinese intelligence services. As the United States upgrades its networks to the next generation of wireless technologies—5G—we cannot ignore the risk that that the Chinese government will seek to exploit network vulnerabilities in order to engage in espionage, insert malware and viruses, and otherwise compromise our critical communications networks.

“The FCC has a part to play in combatting this risk by ensuring that its \$8.5 billion Universal Service Fund does not underwrite national security threats. That's why I have circulated to my

colleagues new rules to ban recipients of FCC funds from doing business with untrusted vendors like Huawei and ZTE. I've also proposed to scrutinize the equipment already in our USF-funded networks and determine how best to provide the financial support required for carriers operating these networks to remove and replace such equipment.”

###

Office of Chairman Pai: (202) 418-1000 / Twitter: @AjitPaiFCC / www.fcc.gov/leadership/ajit-pai

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action. See MCI v. FCC, 515 F.2d 385 (D.C. Cir. 1974).