FCC NEWS from the Federal Communications Commission

Media Contact:
Mark Wigfield, (202) 418-0253
mark.wigfield@fcc.gov

For Immediate Release

FCC BARS USE OF UNIVERSAL SERVICE FUNDING FOR EQUIPMENT & SERVICES POSING NATIONAL SECURITY RISKS

Proposes Process for Removing Prohibited Equipment Already in USF-Funded Networks

WASHINGTON, November 22, 2019—As part of its continuing efforts to safeguard the security and integrity of the nation's communications networks, the Federal Communications Commission has barred use of its $8.5 billion a year Universal Service Fund (USF) to purchase equipment and services from companies that pose a national security threat.

The Order adopted today initially designates Huawei Technologies Company and ZTE Corp. as companies covered by this rule and establishes a process for designating additional covered companies in the future. The Order also establishes a certification and audit regime to enforce the new rule.

In an accompanying Further Notice of Proposed Rulemaking adopted today, the FCC is proposing to require carriers receiving USF funds, known as eligible telecommunications carriers, to remove and replace existing equipment and services from covered companies. The Further Notice also seeks comment on how to pay for such removal and replacement. And to aid in the design of a removal and replacement program, the FCC will conduct an information collection to determine the extent to which eligible telecommunications carriers have equipment from Huawei and ZTE in their networks and the costs associated with removing and replacing such equipment.

Modern communications networks are an integral component of the U.S. economy, enabling the voice, data, and Internet connectivity that fuels all other critical industry sectors—including our transportation systems, electrical grid, financial markets and emergency services. But these networks are vulnerable to various forms of surveillance and attack that can lead to denial of service, and loss of integrity and confidentiality of network services. As the United States upgrades its networks to the next generation of wireless technologies—5G—the risk that secret "backdoors" in our communications networks will enable a hostile foreign power to engage in espionage, inject malware, or steal Americans' data becomes even greater.

Both Huawei and ZTE have close ties to the Chinese government and military apparatus and are subject to Chinese laws requiring them to assist with espionage, a threat recognized by other federal agencies and the governments of other nations. The public funds in the FCC's USF, which subsidizes U.S. broadband deployment and service through four separate programs, must not endanger national security through the purchase of equipment from companies posing a national security risk.

The rule barring purchase of equipment and services from covered companies takes effect immediately upon publication in the Federal Register.

Action by the Commission November 22, 2019 by Report and Order, Further Notice of Proposed Rulemaking, and Order (FCC 19-121). Chairman Pai, Commissioners O'Rielly, Carr, Rosenworcel, and Starks approving and issuing separate statements.

WC Docket No. 18-89

###