

**Media Contact:**

Anne Veigle, (202) 418-0506

anne.veigle@fcc.gov

**For Immediate Release****FCC ADOPTS RULES FOR IDENTIFYING, REMOVING, AND REPLACING COMMUNICATIONS EQUIPMENT AND SERVICES POSING A THREAT TO U.S. NATIONAL SECURITY*****Establishes Program to Fund Replacement of Insecure Equipment and Services***

WASHINGTON, December 10, 2020—The Federal Communications Commission today adopted rules to implement the Secure and Trusted Communications Networks Act of 2019, further protecting the security of the United States and the safety of U.S. communications networks.

Specifically, the Second Report and Order approved today requires the Commission to publish a list of communications equipment and services determined to be a risk to national security that has been identified either by (1) executive branch interagency bodies with appropriate national security experience; (2) the Department of Commerce pursuant to its authority under Executive Order 13873; (3) Congress in the John S. McCain National Defense Authorization Act for Fiscal Year 2019, or (4) U.S. national security agencies. Once Congress appropriates funding, eligible telecommunications carriers that receive universal service funding to provide service in remote areas of the country must remove such equipment or services from their networks and properly dispose of it.

The Order also establishes and adopts rules for the Secure and Trusted Communications Networks Reimbursement Program, which will provide funds to smaller providers of advanced communications services for the removal and replacement of communications equipment and services on the list published by the Commission, conditioned on the appropriation of funds by Congress. Commission staff have estimated the program will require at least \$1.6 billion to reimburse eligible providers, based on an [analysis](#) conducted by the Commission's Wireline Competition Bureau and Office of Economics and Analytics.

The Order further requires all providers of advanced communications services to report whether their networks include any covered communications equipment or services acquired after August 14, 2018. Finally, the Order mandates strict reporting requirements to ensure that the Commission is kept informed about the ongoing presence of insecure equipment in U.S. communications networks.

Today's Order builds on a series of recent actions the Commission has taken to protect U.S. communications network supply chains, including the [November 2019 ban](#) on use of the \$8.3 billion Universal Service Fund to purchase any equipment or services produced by companies that pose a national security threat. In June 2020, the Commission's Public Safety and

Homeland Security Bureau [formally designated](#) Huawei and ZTE, as well as their parents, affiliates, and subsidiaries, as covered companies for purposes of the agency's ban.

The Commission also has taken action to block threats to U.S. communications networks through the denial of authority to provide services in the United States, [declining in 2019](#) to grant China Mobile's application for international Section 214 authority.

Action by the Commission December 10, 2020 by Report and Order (FCC 20-176). Chairman Pai, Commissioners O'Rielly, Carr, Rosenworcel, and Starks approving and issuing separate statements.

WC Docket No. 18-89

###

**Media Relations: (202) 418-0500 / ASL: (844) 432-2275 / Twitter: @FCC / [www.fcc.gov](http://www.fcc.gov)**

*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).*