STATEMENT OF
CHAIRMAN AJIT PAI

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89.

National security experts have warned that when companies are beholden to foreign governments with interests adverse to the United States, their products and services can threaten our country. This is certainly the case with the Chinese telecommunications equipment manufacturers Huawei and ZTE. As Lieutenant General and former National Security Advisor H.R. McMaster recently explained in The Atlantic, China "use[s] . . . major telecommunications companies to control communications networks and the [I]nternet overseas."

This is not surprising. Huawei and ZTE each have close ties to the Chinese Communist Party and China's military, and both companies are broadly subject to Chinese law obligating them to cooperate with the country's intelligence services. With respect to Huawei, McMaster writes, "There should no longer be any dispute concerning the need to defend against . . . Huawei and its role in China's security apparatus." In light of the "incontrovertible evidence of the grave national-security danger associated with a wide array of Huawei's telecommunications equipment," he advises that a policy priority for the United States and its allies should be "the development of infrastructure, particularly 5G communications, to form trusted networks that protect sensitive and proprietary data."

At the FCC, we couldn't agree more. That's why, last fall, the Commission unanimously adopted a ban on the use of universal service support to purchase, obtain, or maintain any equipment or services from companies posing a national security threat to communications networks or the communications supply chain. And last month, the FCC's Public Safety and Homeland Security Bureau formally designated Huawei and ZTE as covered companies for purposes of our November 2019 ban. As a result, the FCC's $8.3 billion a year Universal Service Fund (USF) can no longer be used to underwrite these suppliers.

Today, we take additional steps to protect America's communications networks from national security threats. Specifically, we integrate provisions of the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act), which was enacted in March 2020, into our existing supply chain rulemaking proceeding. We start with a Declaratory Ruling in which we determine that we've already fulfilled one of our new statutory obligations. In particular, we find that by adopting our November 2019 ban on USF support for equipment and services produced or provided by companies that pose a national security threat, we have substantially met our obligation under the Secure Networks Act to prohibit the use of federal subsidies for covered communications equipment and services.

We also adopt a Second Further Notice of Proposed Rulemaking to seek public input on implementing various other parts of the Secure Networks Act. First, we propose ways to create and maintain the list of covered communications equipment and services required by the statute. Second, we propose to ban the use of federal subsidies, including USF funding, for any communications equipment or services placed on this list. Third, we propose to require all providers of advanced communications services to report on whether they use any covered communications equipment or services. Finally, we propose rules to prevent waste, fraud, and abuse in the reimbursement program to remove and replace insecure equipment that Congress has mandated in the Secure Networks Act. We sought comment on this reimbursement program in April 2020, and I hope that Congress will act quickly to appropriate funding for it. Indeed, last fall, we estimated that a removal-and-replacement program could cost up to $2 billion, so this would be a critical step forward.

For their outstanding work to help secure our nation's communications infrastructure, I'd like to thank the following Commission staff: Pam Arluk, Brian Cruikshank, Justin Faulb, Trent Harkrader, Billy Layton, Kris Monteith, Ramesh Nagarajan, Ryan Palmer, and Morgan Reeds of the Wireline Competition Bureau; Malena Barzilai, Ashley Boizelle, Mike Carlson, Tom Johnson, Doug Klein, Rick

Mallen, and Bill Richardson of the Office of General Counsel; Tanner Hinkel, Ken Lynch, Alec MacDonnell, and Steve Rosenberg of the Office of Economics and Analytics; Jeff Goldthorp, Deb Jordan, Nikki McGinnis, Saswat Misra, and Austin Randazzo of the Public Safety and Homeland Security Bureau; Chrysanthos Chrysanthou, Martin Doczkat, Michael Ha, Ira Keltz, Aspa Paroutsas, and Sean Yun of the Office of Engineering and Technology; and Maura McGowan of the Office of Communications Business Opportunities.

I'd also like to thank the bipartisan group of Representatives and Senators who led efforts to pass the Secure Networks Act, including Chairman Wicker, Senator Warner, Chairman Pallone, and Ranking Member Walden. Thanks as well to Senators Cotton and Rubio for highlighting this issue. All of these efforts are helping make our communications networks safer, and I look forward to continuing to work with them on this national priority.