STATEMENT OF
CHAIRMAN AJIT PAI

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

Last year, testifying before Congress, FBI Director Chris Wray said, "[W]e're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks that provides the capacity to exert pressure or control over our telecommunications infrastructure."[1]

And last week, Attorney General Bill Barr wrote to us:

> [W]e are at a critical moment of technological change. Telecommunications providers in America and around the world are deciding who should build and service the Fifth Generation (5G) of wireless networks. We will become even more dependent on those networks as more and more devices and services are connected and operate at unprecedented speeds. Human life and safety as well as critical government functions will ride on them. Our national defense will depend on the security of our allies' networks as well as our own. Protecting our networks (rural and urban alike) from equipment or services offered by companies posing a threat to the integrity of those networks is therefore a vital national security goal.[2]

At the FCC, we couldn't agree more with the Attorney General and the Director of the FBI. That's why today, we adopt a ban on using funds from the FCC's Universal Service Fund (USF) to purchase equipment or services from companies posing a national security threat to the integrity of communications networks or the communications supply chain. We also initially designate two Chinese companies—Huawei and ZTE—as "covered" companies for purposes of this rule, and we set up a process for designating additional such companies in the future.

We take these actions based on evidence in the record as well as longstanding concerns from the executive and legislative branches about the national security threats posed by certain foreign communications equipment manufacturers, most particularly Huawei and ZTE. Both companies have close ties to China's Communist government and military apparatus. Both companies are subject to Chinese laws broadly obligating them to cooperate with any request from the country's intelligence services and to keep those requests secret. Both companies have engaged in conduct like intellectual property theft, bribery, and corruption.

Moreover, we know that hidden "backdoors" to our networks in routers, switches, and other network equipment can allow a hostile adversary to inject viruses and other malware, steal Americans' private data, spy on U.S. companies, and more. Indeed, just last month, the European Union found 5G security risks where a "hostile state actor exercises pressure over a supplier under its jurisdiction to provide access to sensitive network assets through (either purposefully or unintentionally) embedded vulnerabilities."[3]

---

[1] Hearing before the Senate Select Committee on Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community," 115th Cong. (Feb. 13, 2018) (statement of Christopher Wray, Director, FBI), https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-0#.

[2] Letter from William P. Barr, Attorney General, to Ajit Pai, Chairman, FCC, WC Docket No. 18-89, at 1 (Nov. 13, 2019), https://ecfsapi.fcc.gov/file/111501201939/18-89A.pdf.

[3] European Union, "EU coordinated risk assessment of the cybersecurity of 5G networks" at 27 (Oct. 2019), https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf.

These concerns are by no means hypothetical. This summer, for example, an independent cybersecurity firm found that over half of the Huawei firmware images they analyzed had at least one potential backdoor and that each Huawei device they tested had an average of 102 known vulnerabilities.[4] Similarly, in March 2019, an oversight board in the United Kingdom released a report identifying "[f]urther significant technical issues . . . in Huawei's engineering processes, leading to new risks in the UK telecommunications networks."[5] It also said that it "has not yet seen anything to give it confidence in Huawei's capacity to successfully complete the elements of its transformation program that it has proposed as a means of addressing these underlying defects."[6] It is unsurprising, then, that in the last 12 months, three of our closest allies—New Zealand, Japan, and Australia—have issued bans on Huawei equipment and that over 30 nations (including the U.S.) have embraced a risk-based framework called the Prague Proposals.[7]

Given the threats posed by Huawei and ZTE to America's security and our 5G future, this FCC will not sit idly by and hope for the best. Today, we not only ensure that the federal funds in the USF are not spent on equipment or services from these suppliers, but we also propose a process to remove such equipment already deployed in USF-funded networks. Specifically, we propose to require certain carriers receiving USF funds, known as eligible telecommunications carriers, to remove from their networks existing equipment from covered companies, starting with Huawei and ZTE. To mitigate the financial impact of this requirement, particularly on small, rural carriers, we propose to establish a reimbursement program to help offset the cost of transitioning to more trusted vendors.

Finally, to aid the design of a removal and replacement program, we require carriers to submit information on their use of equipment from Huawei and ZTE as well as the potential costs associated with removal and replacement of such equipment.

In taking these steps, we demonstrate the FCC's commitment to doing everything we can within our statutory authority to address national security threats to our communications networks, and together with our federal partners, to secure our 5G future.

For their outstanding work on this item, I'd like to thank Callie Coker, Kate Dumouchel, Justin Faulb, Ellen Gardiner, Aaron Garza, Trent Harkrader, Billy Layton, Kris Monteith, Ryan Palmer, Gilbert Smith, Cody Venzke, and John Visclosky of the Wireline Competition Bureau; Kenneth Baker, Erin Boone, Garnet Hanley, Kari Hicks, Charles Mathias, Dana Shaffer, Sean Spivey, Donald Stockdale, Joel Taubenblatt, and Suzanne Tetreault of the Wireless Telecommunications Bureau; Steven Carpenter, Michael Connelly, Lisa Fowlkes, Jeffrey Goldthorp, Kurian Jacobs, Debra Jordan, Lauren Kravetz, Nicole McGinnis, Saswat Misra, and Austin Randazzo of the Public Safety and Homeland Security Bureau; Denise Coca, Kathleen Collins, Gabrielle Kim, David Krech, Arthur Lechtman, Thomas Sullivan, and Troy Tanner of the International Bureau; Rosemary Harold, Christopher Killion, Shannon Lipp, and Jeremy Marcus of the Enforcement Bureau; Ira Keltz, Julius Knapp, Aspasia Paroutsas, and Ronald Repasi of the Office of Engineering and Technology; Malena Barzilai, Michael Carlson, Thomas Johnson, Douglas Klein, Rick Mallen, Linda Oliver, and Bill Richardson of the Office of General Counsel; Maura McGowan and Sanford Williams of the Office of Communications Business

[4] "Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd." at 3 (June 2019), https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf.

[5] "Huawei Cyber Security Evaluation Center (HCSEC) Oversight Board Annual Report 2019: A report to the National Security Adviser of the United Kingdom" at 2 (Mar. 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

[6] *Id.* at 3.

[7] *See* "Prague 5G Security Conference announced series of recommendations: The Prague Proposals" (May 3, 2019), https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

Opportunities; and Eric Burger, Octavian Carare, Jim Eisner, Kenneth Lynch, Alec MacDonnell, Giulia McHenry, Chuck Needy, Eric Ralph, Steven Rosenberg, Craig Stroup, Emily Talaga, and Geoff Waldau of the Office of Economics and Analytics.