STATEMENT OF
CHAIRMAN AJIT PAI

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

America's communications networks have become the indispensable infrastructure of our economy and our everyday lives. That makes safeguarding those networks vitally important to our national security, economic security, and personal security. An important part of that security is the integrity of the communications supply chain—that is, the process by which products and services are manufactured, distributed, sold, and ultimately integrated into our networks.

For years, U.S. government officials have expressed concern about the national security threats posed by certain foreign communications equipment providers in the communications supply chain. Hidden "backdoors" to our networks in routers, switches, and other network equipment can allow hostile foreign powers to inject viruses and other malware, steal Americans' private data, spy on U.S. businesses, and more.

These threats persist today. Just two months ago, the Director of the Federal Bureau of Investigation testified before Congress about the "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."[1] These risks include "the capacity to maliciously modify or steal information" and "conduct undetected espionage."[2] And according to the Director of the National Security Agency, "this is a challenge that . . . is only going to increase, not lessen, over time for us."[3]

To be sure, the FCC doesn't have the authority or capacity to solve this problem alone. But it does have a role to play in meeting this challenge. Specifically, given the Commission's responsibility for overseeing the almost $9 billion Universal Service Fund (USF), we must ensure that the money in the USF—which comes from fees paid by American consumers—isn't used in a way that undermines our national security. And we must take this action now, especially as we stand upon the precipice of the 5G future.

That's why we're proposing a rule that, going forward, prohibits universal service support from being used to purchase or obtain any equipment or services produced or provided by any company posing a national security threat to communications networks or the communications supply chain. We seek public input on how best to implement this proposal, including the costs and benefits of doing so. We also ask what types of equipment and services should be covered by the proposed rule, how we should identify which suppliers are covered, and how USF recipients can learn who those suppliers are. I am confident that the record we compile will allow us to do our part to help protect America's national security.

This *Notice* was clearly a team effort. I would therefore like to thank the following staff across the Commission's Bureaus and Offices: Liz Drogula, Madeleine Findley, Aaron Garza, Jodie Griffin, Christian Hoefly, Daniel Kahn, Radhika Karmarkar, Alex Minard, Kris Monteith, Ramesh Nagarajan, Ryan Palmer, Eric Ralph, and John Visclosky of the Wireline Competition Bureau; Charles Mathias, Aalok Mehta, Dana Shaffer, and Don Stockdale of the Wireless Telecommunications Bureau; Chris

---

[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-hearing-1 at 02:06:50 – 02:08:00.

[2] *Id*.

[3] *Id*. (statement of Admiral Michael Rogers, Director, NSA), https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-hearing-1 at 02:08:06 – 02:08:13.

Anderson, Merritt Baer, Justin Cain, Lisa Fowlkes, Jeff Goldthorp, Deb Jordan, Nikki McGinnis, Vern Mosley, Anita Patankar-Stoll, and David Plotinsky of the Public Safety and Homeland Security Bureau; David Krech, Thomas Sullivan, and Troy Tanner of the International Bureau; Rosemary Harold and Keith Morgan of the Enforcement Bureau; Ashley Boizelle, Tom Johnson, Doug Klein, Frank Inserra, Rick Mallen, Linda Oliver, Bill Richardson, and Chin Yoo of the Office of General Counsel; Maura McGowan of the Office of Communications Business Opportunities; Kevin Holmes, Jennifer Schneider, and Tim Strachan of the Office of Legislative Affairs; Deena Shetler and Mark Stephens of the Office of Managing Director; and Jerry Ellig, Paul Lafontaine, and Wayne Leighton of the Office of Strategic Planning and Policy Analysis.

I'm also grateful to the bipartisan group of Senators and Representatives that has urged the FCC to take action on this issue. Led by Senator Tom Cotton, these members have been strong advocates for protecting our communications networks from national security threats, and I look forward to working with them toward that goal.