STATEMENT OF
ACTING CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program,* ET Docket No. 21-232; *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, EA Docket No. 21-233.

Our 5G future is about connecting everything. It is about moving to a new networked world that will open up possibilities for communications that we cannot even fully imagine today. By exponentially increasing the connections between people and things around us, this technology could become an input in everything we do—improving agriculture, education, healthcare, energy, transportation, and more. The data we derive from all these connections is powerful. It will inform machine learning, artificial intelligence, and the next generation of innovation across the economy.

But to get there from here requires us to rethink our communications supply chain. That's because insecure network equipment can undermine our 5G future, providing foreign actors with access to our communications. This, in turn, may mean the ability to inject viruses and malware in our network traffic, steal private data, engage in intellectual property theft, and surveil companies and government agencies.

To address this risk, the Federal Communications Commission is now pursuing a proactive, three-pronged strategy to build a more secure and resilient communications supply chain for our 5G future. We are taking direct action to exclude untrusted equipment and vendors from communications networks both at home and abroad. We are recognizing that "Just Say No" is not a strategy, so we are moving fast to speed the way for trustworthy innovation. We are also engaged in a multifaced effort across government, with industry, and with partner nations to protect our networks from threats.

Today, I am pleased that we are kicking off a rulemaking and inquiry that will spark new progress on each of these three lines of effort.

First, we consider new measures to exclude untrustworthy equipment from our communications networks. To date, the FCC has prohibited the use of support from our universal service fund to purchase equipment that could pose a national security threat to the United States. Under the law, this includes communications equipment and services from Huawei, ZTE, Hytera, Hikvision, and Dahua. Thanks to the Secure and Trusted Communications Networks Act and a $1.9 billion appropriation from Congress, we also are putting the finishing touches on a program to replace insecure network equipment from these vendors to the extent that it is present in our domestic networks today. At the same time, we've taken action to ensure that foreign telecommunications companies that obtain or seek access to the market in the United States do not present a national security threat.

So far, so good. But today we go further. Because it does not make sense to have these bans in place but leave open other opportunities for this equipment to reach our markets and be present in our networks. Yet that is exactly the state of our rules today. Despite having identified security concerns with telecommunications equipment from Huawei and ZTE back in 2019, for the last several years this agency has continued to put its stamp of approval on this equipment. In other words, we have left open opportunities for its use in the United States through our equipment authorization process. So here we propose to close that door.

This is common sense. It will better align our equipment authorization procedures with our national security policies. It means the FCC would no longer approve equipment that is identified under

the Secure and Trusted Communications Networks Act as posing an unacceptable risk to the national security of the United States or the safety of United States persons. To round this effort out, we also seek comment on a number of other proposals designed to ensure that insecure equipment is not present in our networks.

Second, we continue to speed the way for trustworthy innovation. By reducing our dependence on network components developed by untrusted vendors, we send a strong signal that the United States is committed to developing a market for secure 5G equipment alternatives. To this end, our ongoing work to foster the development of open radio access networks is important. Because if we do this right we will have a renewed opportunity for American technology leadership, more competition, better economic security, more resiliency in our supply chains, and improved ability to protect the privacy and data of citizens.

Thanks to my colleague Commissioner Starks, we also ask questions about how the United States participates in standards-setting organizations. These bodies can play a big role in shaping the growth of future technologies. That means it is in our national interest to ensure that these organizations operate in a fair, impartial, balanced, and consensus-based manner and in accordance with fundamental rules of due process. That is why I have made the FCC's participation a priority—to ensure that we are contributing our technical expertise and keeping our innovative edge. In fact, under my leadership, I am pleased to announce that the FCC has increased the number of our staff dedicated to standards development issues by more than 50 percent. I believe it is imperative that the United States government invest the resources necessary to lead in these processes because when we do we lead the world by example.

Third, we explore how we can advance a multifaceted, strategic approach to protect our networks from all threats. The United States had 65,000 ransomware attacks last year. If you do the math, that is seven every hour. One recent attack shut down a key pipeline and emptied many gas stations across the Southeast. Another attack raised fears about the domestic beef supply. What started as a nuisance has quickly become a national security problem as cybercriminals target key parts of our infrastructure.

These events remind us that we need to think about security in everything we do in our connected world. As part of this effort, we need to acknowledge that the equipment that connects to our networks is just as consequential for our national security as the equipment that goes into our networks. That means focusing on network equipment and supply chain security is not enough. We also need to focus on the security of the connected things—otherwise known as the Internet of Things.

That is why in our inquiry today we ask questions about how we can leverage our equipment authorization procedures to encourage device manufacturers to build security into new connected products. We ask how we can build on existing efforts at the National Institute of Standards and Technology or elsewhere to do it. The time to have this discussion is now—because our cybersecurity challenges will only grow as connections multiply and the Internet of Things expands.

I look forward to the record that develops. The policies we propose and the questions we ask are a big step toward renewing trust in our communications networks and trust in our equipment authorization system. They demonstrate that the FCC is committed to doing everything we can, together with our federal partners, to support the security of our communications networks. Our proposals also would implement the provisions of the Secure Equipment Act of 2021, and I thank Senator Markey, Senator Rubio, Congresswoman Eshoo, and House Republican Whip Steve Scalise for their leadership on these issues.

Thank you also to the staff that worked on this effort, including Brian Butler, Jamie Coleman, Martin Doczkat, Howard Griboff, Michael Ha, Ira Keltz, Muli Kifle, Paul Murray, Siobahn Philemon, Jamison Prime, Ron Repasi, Dana Shaffer, Rodney Small, Tom Struble, Jim Szeliga, George Tannahill, Alfonso Tarditi, Dusmantha Tennakoon, and Ron Williams from the Office of Engineering and Technology; Jonathan Campbell, Giulia McHenry, Chuck Needy, Erik Salovaara, Michelle Schaefer, Deena Shetler, and Emily Talaga from the Office of Economics and Analytics; Matthew Dunne, David Horowitz, Doug Klein, Jacob Lewis, and Bill Richardson from the Office of General Counsel; Gabriel Collazo, Jeffrey Gee, Pamela Kane, Chris Killion, Jason Koslofsky, Shannon Lipp, Jeremy Marcus, Neil McNeil, Elizabeth Mumaw, Phillip Rosario, Raphael Sznajder, and Ashley Tyson from the Enforcement Bureau; Denise Coca, Thomas Sullivan, and Kathy O'Brien from the International Bureau; Ronald Cunningham, Debra Jordan, Lauren Kravetz, Nikki McGinnis, Zenji Nakazawa, and Austin Randazzo from the Public Safety and Homeland Security Bureau; Brian Cruikshank, Elizabeth Cuttner, and Justin Faulb from the Wireline Competition Bureau; Jessica Greffenius, Kari Hicks, Charles Mathias, and Joel Taubenblatt from the Wireless Telecommunications Bureau; and Maura McGowan from the Office of Communications Business Opportunities.