STATEMENT OF
ACTING CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Promoting the Deployment of 5G Open Radio Access Networks*, GN Docket No. 21-63

Today the Federal Communications Commission is launching the first-ever inquiry exploring how we can accelerate the development and deployment of open radio access networks for 5G in the United States.

This is important because 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 building this future right means building security in front from the start. That's because this new endless connectivity also means new vulnerabilities. With so much on the line, it's urgent that trustworthy companies build the next-generation networks that will soon touch so much of our lives. And it's critical that we not give control of our important infrastructure to untrusted vendors like Huawei or ZTE.

Right now, that is easier said than done. To understand why, start with history. The United States invented the telecommunications equipment industry. Not all that long ago we dominated it. But in recent years the industry has shifted as American companies were acquired and consolidated into European players. At the same time China ramped up its national strategy to produce new network equipment. While these efforts began at the lower end of the market, they are now clearly focused on global 5G deployment.

This means we have a supply chain challenge. We have only four major vendors for mobile network equipment to choose from, none of which hails from the United States. Plus, the vendors that have grown fastest in recent years are from China, in part because the Chinese government deploys powerful industrial policies to make their equipment cheaper to deploy than the alternatives. We know based on a comprehensive record developed by various national security agencies around the world that there are serious risks that come with having this equipment in our networks—and these vulnerabilities could provide foreign interests with the ability to jeopardize the security of communications in the United States.

The good news is we are taking direct action to slow down untrusted vendors both at home and abroad. Thanks to the Secure and Trusted Communications Networks Act, we are putting the finishing touches on a system to replace insecure equipment from Chinese companies like Huawei and ZTE, to the extent that it is present in our domestic networks today. Thanks to initiatives like the Prague Principles, we have a foundation for working with like-minded countries to promote international policies that enable secure and trusted 5G supply chains.

This is good. But there is another strategy that needs our attention too. While we continue to take action to slow down untrusted vendors, *we also must take action to speed up American innovation*.

This is what today's effort is all about. At the FCC we are starting the first-ever inquiry into open RAN. Today, the RAN is the most restrictive and most expensive part of the network, in part because all of its major components have to come from the same vendor. There is no way to mix and match. But if

we can unlock the RAN and diversify the equipment in this part of our networks, we may be able to increase security, reduce our exposure to any single foreign vendor, lower costs, and push the equipment market to where the United States is uniquely skilled—in software.

That sounds promising. And as a result of our effort today, we will have the first comprehensive record on the public interest benefits of new interoperability in the RAN. We will have the first assessment of the state of this technology, how our rules may be adjusted to foster its growth, and how our coordination with other federal actors—from the National Science Foundation to the Department of Defense—may stimulate its development in the marketplace.

At the same time, we do not shy away from the hard questions. We ask about challenges associated with systems integration and management. We consider reliability and quality of service. We ask whether new openness also could introduce new vulnerabilities to the network. These questions are important to understand whether open RAN will deliver on its national security promise.

This inquiry is important. It is also overdue. It was nearly two years ago that I was the first at the FCC to speak about the power of open RAN. I was drawn to this technology because it has the potential to address our security needs and supply chain challenges.

I believed back then what I believe now—we should be exploring how government policies can help kickstart the development of open RAN. That's because expanding opportunities for software-centric architectures deeper in our networks could yield communications with more security, lower costs, and greater innovation. It is how we can lead once more in the market for network equipment—and build our 5G future from a position of strength.

Thank you to the agency staff for their work on this Notice of Inquiry. From the Wireless Telecommunications Bureau that's Thomas Derenge, Charles Mathias, Roger Noel, Paul Powell, Kambiz Rahnavardy, Jaclyn Rosen, Catherine Schroeder, Sean Spivey, Joel Taubenblatt, and Mary Claire York. From the International Bureau that's Ena Dekanic, Olga Madruga-Forti, Roxanne McElvane Webber, Andrew Pegues, Jim Schlichting, Thomas Sullivan, and Michele Wu-Bailey. From the Public Safety and Homeland Security Bureau that's Eric Burger, Lisa Fowlkes, Jeff Goldthorp, Debra Jordan, and Zenji Nakazawa. From the Wireline Competition Bureau that's Pamela Arluk, Brian Cruikshank, Justin Faulb, Trent Harkrader, Billy Layton, and Kris Monteith. From the Office of Economics and Analytics a thank you to Patrick DeGraba, Cher Li, Catherine Matraves, Giulia McHenry, Michelle Schaefer, Donald Stockdale, and Patrick Sun. From the Office of Engineering and Technology a thank you to Martin Doczkat, Monisha Ghosh, Michael Ha, Ira Keltz, Nicholas Oros, Robert Pavlak, Ronald Repasi, Dana Shaffer, and Sean Yun. From the Office of General Counsel a thank you to David Horowitz, Douglas Klein, and William Richardson. Last but not least, from the Enforcement Bureau thank you Matt Gibson, Janet Moran, and Axel Rodriguez.