STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL

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

We live in a world gone wireless. Our future will be built on 5G infrastructure. So we need to ensure that infrastructure is safe—and that begins with keeping insecure equipment out of our networks.

Today the Federal Communications Commission helps do just that by acting at the direction of Congress to implement the Secure and Trusted Communications Networks Act. This law prohibits the use of public funds to obtain communications equipment or services from a company that poses a national security risk. In addition, it requires the FCC to maintain a list of "covered communications equipment or services" that could undermine our national security and it authorizes a program to reimburse the cost of replacing prohibited equipment.

But take note, because this is only one action in a series taken by this agency to keep insecure equipment out of our nation's communications networks. Two years ago, the FCC first sought comment on supply chain issues and proposed a rule to prohibit the use of universal service funds to purchase equipment and services from providers that may pose a security risk. Last year, we adopted this rule. Then we started an information collection to survey where insecure equipment is in our networks and estimate the cost to remove it. We also denied an application from China Mobile to enter our markets and put four other similarly situated companies on notice they could share the same fate. Last month we designated two Chinese companies—Huawei and ZTE—as national security threats because the evidence suggests the Chinese government could exert control over them. It is clear the world is watching. Because just this week the United Kingdom announced it, too, will bar its networks from using 5G equipment made by untrusted providers.

In the instant decision, we find that our efforts last year prohibiting the use of universal service funds to support the purchase of insecure equipment and services largely satisfy our obligations under Section 3 of the Secure and Trusted Communications Networks Act. Then in the rulemaking we seek comment on how to implement the remaining aspects of this law. Over time, I hope we can do more to harmonize the processes we established last year with those required in this new law. I also hope we can explore how existing law—from the Communications Act to the Communications Assistance for Law Enforcement Act—can bolster those efforts. So today's decision and rulemaking has my support.

But let's not stop here. Because there is more we can do to secure our 5G future. There is more we can do to power the future of innovation. There is more we can do to make sure the United States has a fighting chance at leading in what comes next.

That begins with fixing our obvious missteps. Those include suspending new work visas for a wide variety of technology jobs and deterring foreign students from studying and staying on our shores—something the President of the Massachusetts Institute of Technology has said fuels our "persistent advantage in scientific creativity." Likewise, we need to be mindful how increased consolidation in our economy impacts what innovations make it to market and get the opportunity to change our world.

Closer to home, we need the FCC to do more than just ban the presence of Chinese companies. Because this is not about retribution. It is about building a better future. If we want to ensure no equipment provider can undermine our communications, we need the United States to spur a new and more innovative and diverse ecosystem of secure equipment and equipment providers. I think the FCC can help do that.

A year ago, at a gathering of Mobile World Congress Americas, I was the first to call on the FCC to help develop a more secure communications future by supporting open radio access networks—or open RAN. The RAN is the part of the network that sits between your device and the network core. It is the

most expensive and restrictive part of the network today. All major components of a RAN have to come from the same vendor—there is no way to mix and match.

When I offered this idea, no companies based in the United States were manufacturing 5G equipment for this part of our networks—thanks in part to a long history of consolidation in the sector. Meanwhile, Chinese companies were selling nearly half of all global RAN gear. The security risks inherent in this state of affairs are easy to understand.

So I suggested that we do something to reverse these trends. I suggested that if we can unlock the RAN by virtualizing this part of our network, we could help spur a market for more secure 5G equipment. We could expand the number of suppliers, promote the long-term viability of the 5G supply chain, and prevent growing dependence on Chinese vendors. Even better, this effort could push the market for 5G equipment to the sectors where the United States is strongest: in software and semiconductors.

I got the chance to talk more about this when I testified before the Senate Committees on Homeland Security and Government Affairs and Commerce, Science, and Transportation. In recent months, it has garnered support from my colleagues at the FCC too. It is a recurring theme in comments to the National Telecommunications and Information Administration on the National Strategy to Secure 5G Implementation Plan. And it has been embraced by more than 30 companies that have joined the Open RAN Policy Coalition.

This is progress. But here is what we need to do next.

First, we need a whole-of-government approach to advancing open RAN in the United States. Right now, we don't have it. The Attorney General recently called this effort "just pie in the sky." He's not right. It may be audacious, but that's exactly why the United States needs to lead. Yet there are reports that the Department of State wants a watered-down version of the open RAN concept. This is troubling. Across the board we need a more cohesive government-wide 5G strategy, especially with open RAN.

Second, we need to develop testbeds in the United States that bring together a mix of stakeholders interested in developing and promoting open RAN. As I've said before, the FCC can build this into our ongoing effort to authorize city-wide 5G testbeds in New York and Salt Lake City. But to date we haven't done so. In the meantime, the United Kingdom is working on 5G testbeds to support open RAN, the European Union is boosting investment in 5G equipment innovation, and a Japanese company has already deployed a commercial mobile network using open RAN. Plus, the Department of Defense is working on 5G testbeds that will include open RAN architectures. I think the FCC should support testbeds for the commercial development of this capability, too.

Third, the we need to task the FCC's Communications Security, Reliability, and Interoperability Council with identifying impediments to open RAN development in the United States and what new efforts can be undertaken to support secure and interoperable equipment. It already has a charter to consider security risks in emerging 5G networks. We need to expand it to explore this technology. Similarly, when the FCC participates in standards-setting bodies like 3GPP and the Alliance for Telecommunications Industry Solutions, we should consider how we can support the goals of openness and interoperability.

Fourth, we need resources to make this all happen. For starters, we need an appropriation from Congress for the reimbursement program created by the Secure and Trusted Communications Networks Act. But solving our security challenges in the present is not enough. So I hope Congress proceeds with the Utilizing Strategic Allied Telecommunications Act, which would fund research and development for a secure wireless supply chain. The odds are good. Because just this week the Energy and Commerce Committee advanced this legislation to the full House of Representatives. In addition, elements of the Senate version of this bill have been included in the Intelligence Authorization Act, demonstrating just how powerful these matters are for national security both at home and abroad.

All of these efforts would help our supply chain challenges today and more importantly, assist with the development of a more secure and innovative future. We need to remember we cannot limit our focus to keeping untrusted companies and Chinese equipment out of our networks. We need a vibrant and diverse set of trusted equipment and companies in their place, and the United States should help lead the development of this new communications ecosystem. The most important thing is that we get started right now.