STATEMENT OF
JESSICA ROSENWORCEL
COMMISSIONER
FEDERAL COMMUNICATIONS COMMISSION
BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
WASHINGTON, D.C.
OCTOBER 31, 2019

Good morning, Chairman Johnson, Ranking Member Peters, and Members of the Committee. Thank you for the opportunity to appear before you today.

For the last decade, the United States has led the world in wireless technology and performance, and we have reaped the benefits. The smartphone revolution began here on our shores. The new world of wireless it fostered fueled economic growth at home and abroad. It helped secure our global dominance in the technology sector.

Let me be blunt. That authority is now being challenged. Extending this leadership into the next generation of wireless technologies—5G—is going to be difficult. But it's worth the effort. With speeds as much as 100 times faster than present networks and much lower latency, these networks will kickstart the next big digital transformation. By connecting many more things in many more places, 5G offers new ways to foster economic activity and improve health, education, the environment, and more. In short order, the smartphone could become the least innovative thing about our wireless world.

However, earlier this year the Defense Innovation Board—the United States military's premier advisory board of academic researchers and private sector technologists—surveyed the state of next-generation 5G networks and issued a sober warning. They found that "the country that owns 5G will own innovations and set the standards for the rest of the world," and "that country is currently not likely to be the United States."

This is a clarion call. Other nations saw very clearly the success in the United States with the last generation of wireless technology and are working overtime to ensure that they secure a leadership position—and their efforts are bearing fruit.

We see it in deployment. Switzerland has more commercial 5G deployments than any other country. South Korea has led the world in bringing a mix of high-band and mid-band spectrum to auction to support 5G service. China, Germany, and Japan have built out more infrastructure on a per capita basis to carry 5G airwaves.

We see it in activity in standards bodies. Countries are amassing bigger delegations and submitting more proposals at international fora, like 3GPP and the International Telecommunication Union, where 5G specifications are being hammered out.

We see it in patents and equipment. Based on recent reports, Chinese companies own 36 percent of all 5G standard-essential patents—more than double their share of 4G patents—setting themselves up for big royalties ahead. Companies in the United States today, by contrast, hold just 14 percent. In fact, there are no longer any United States-based manufacturers of key 5G network equipment.

The truth is we are facing well-resourced challenges to our 5G leadership from every direction. And so far, we do not have a comprehensive national plan in place with a fully coordinated interagency response to meet that challenge.

We need one—and here are four ideas it should include.

First, if we want to lead in 5G, we have to secure the 5G supply chain. The underlying truth about next-generation communications networks in many parts of the world is that technology developed in China will be at the center. This threatens to expose our networks and our most private data to undue foreign influence.

The good news is we are making some progress with our federal networks. The Pentagon has banned the sale of insecure Chinese equipment on military bases. In addition, the National Defense Authorization Act prohibits federal agencies from using this equipment. But when it comes to our commercial networks, we are still woefully behind. At the Federal Communications Commission we have a rulemaking to ensure that our universal service fund, which provides billions annually to support broadband deployment in rural communities, going forward will not be used to purchase insecure network equipment. That rulemaking has inexplicably stalled for more than a year and a half. But now, perhaps because you announced this hearing, we have publicized that we will vote on this in three short weeks.

Second, we need an approach to supply chain security that recognizes that despite our best efforts, secure networks in the United States will only get us so far because no network stands by itself. Our networks still will connect to insecure equipment abroad. So we need to start researching how we can build networks that can withstand connection to equipment vulnerabilities around the world. One way to do this is to invest in virtualizing radio access networks—or open RAN. The RAN is the most expensive and restrictive part of the network—it sits between your device and a carrier's core network. Today, all major components of a RAN 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 can increase security and push the market for equipment to where the United States is strongest—in software and semiconductors. This also will give carriers around the world that are locked into upgrade cycles with a single foreign vendor a way out.

Third, we need smarter spectrum policy. To date, the FCC has aggressively focused its early efforts to support 5G wireless service by bringing only high-band spectrum to market. This is a mistake. The rest of the world does not have this singular early focus on high-band, millimeter airwaves, with good reason. These airwaves have substantial capacity but their signals do not travel far and are easily blocked by walls. As a result, commercializing them is costly—especially in rural areas. The sheer volume of antenna facilities required to make this

service viable will limit deployment to the most populated urban areas. This means our early 5G spectrum policy could create 5G haves and have-nots, deepening the digital divide that already plagues too many rural communities nationwide. That's not right. If you care about rural broadband, this matters. The FCC needs to change course and make it a priority to auction mid-band spectrum, which has a mix of capacity and propagation which is better suited to extend the promise of 5G wireless service to everyone, everywhere in the country.

Fourth and finally, with 5G we are moving to a world with billions of connected devices around us in the internet of things. We need to adjust our policies now to ensure this future is secure. After all, the equipment that *connects* to our networks is just as consequential for security as the equipment that goes *into* our networks.

Here is what that could look like. Every device that emits radiofrequency at some point passes through the FCC. If you want proof, pull out your smartphone or take a look at the back of any computer or television. You'll see an identification number from the FCC. It's a stamp of approval. It means the device complies with FCC rules and policy objectives before it is marketed or imported into the United States. This routine authorization process takes place behind the scenes. But the FCC needs to revisit this process and explore how it can be used to encourage device manufacturers to build security into new products. To do this, we could build on the National Institutes of Standards and Technology draft set of security recommendations for devices in the internet of things. This effort specifies the cybersecurity features to include in network-capable devices, whether designed for the home, hospital, or factory floor. It covers everything from device identification, device configuration, data protection, access to interfaces, and critical software updates. In other words, it's a great place to start—and we should do it now.

Chairman Johnson, Ranking Member Peters, and Members of the Committee, thank you once again for holding this hearing. Thank you for providing me with the opportunity to offer my views. I look forward to answering any questions you have.