REMARKS OF
COMMISSIONER JESSICA ROSENWORCEL
5G SECURITY RURAL ENGAGEMENT INITIATIVE
FLOWOOD, MISSISSIPPI
NOVEMBER 20, 2019

Good morning. It's great to join you in Mississippi for the 5G Securing Rural Engagement Initiative. Throughout the country there is a fierce focus on what we need to do to secure our 5G future—and I'm here today because I believe rural communities and small businesses will play an important part in that effort.

In fact, on Friday this week the Federal Communications Commission will vote to adopt a rule ensuring that our universal service funds—which provide billions annually to support broadband deployment in rural communities—are not used to purchase insecure network equipment. We also will kick off a rulemaking to identify where this equipment is in networks today and how to help carriers serving rural America replace it.

Let me start today by offering my big picture support to these efforts. I believe it is not enough for the United States to be first to the next-generation of wireless technology—the networks we deploy must also be secure.

But I also believe we need—and our carriers deserve—rules and policies that work in the real world. That's why I've sought changes to what we will consider on Friday. I think with a few changes we can better protect the integrity of our networks and offer more certainty and predictability for carriers.

As a starting point, I believe cybersecurity should be everyone's shared goal—and not just a burden borne by small and rural companies who depend on our universal service programs to bring the possibilities of mobile broadband to rural America. So I've asked that we explore the authority we have to expand our efforts to carriers beyond those using universal service funds. To this end, I have asked the agency to consider how the Communications Assistance for Law Enforcement Act may provide the FCC with the authority it needs to do so.

Then we need to take the lessons we learned about replacing and reimbursing equipment in the wake of the 600 MHz broadcast incentive auction and apply them to the effort to replace equipment that may be insecure. Remember that when Congress authorized the FCC to conduct the broadcast incentive auction, it required the agency to reimburse a range of equipment costs incurred by incumbents. But before making the authorized funds available, the FCC required the eligible entities to certify to the agency basic information about their existing equipment and detailed cost estimates for replacement. Then the FCC conducted audits, data validations, and site visits to ensure the accuracy of the information submitted. To ensure transparency, the FCC made certain equipment eligibility, cost, and disbursement information available to the public. These measures helped maximize the funds available for reimbursement and reduced waste, fraud, and abuse. I believe this effort could serve as a model for the removal of insecure equipment and I've sought changes to include them here, too.

We also need to be careful to ensure that the actions we take on Friday will not needlessly disrupt service in rural America. Companies that will be subject to our new rules need clarity and predictability so that they can continue the day-to-day maintenance, support, and operation of their existing networks in ways that do not compromise the security of American communications. So I've asked that we include examples that would give companies the real-world guidance they need to comply with our rules and avoid unnecessary service disruption.

Finally, I've sought to accelerate the agency's review of the issues posed in the rulemaking regarding a reimbursement program to cover the costs of replacing insecure equipment. The actions we take on Friday will only start the clock. Companies deserve to know what help they have in that effort—and they deserve to know it sooner rather than later. It took us 18 months to reach this point at the FCC, carriers can't wait that long again.

That's a lot. So let me back up and start from the beginning. And just like in the real world, it all starts with the supply chain. The FCC's upcoming vote is a first step, but we have many more steps to take for our networks to be secure in the future. So I want to head beyond our near-term efforts regarding equipment and removal and talk about how in the long-term we can make our networks and our digital world more secure. And I want to talk about how we can use the advent of 5G to do just that.

So here goes three ideas for cybersecurity and the FCC going forward.

First, if we want to lead in 5G, we have to secure the 5G supply chain—and think big about the future when we do.

Let's start this discussion by acknowledging a hard truth: next-generation networks in many parts of the world will have technology developed by China at the center. Right now there is no American company producing some of the most essential 5G equipment. On top of that, the universe of vendors outside the United States is quickly diminishing. Consider that at the turn of the century there were 13 equipment vendors vying to serve carriers. In the run up to 4G that number was down to seven. Now as we embark on 5G, there are only a handful and for some 5G equipment the only options may be from China. Let me add here that the FCC's decision to further consolidate the wireless market in the United States is not going to help this trend because it makes it harder to induce new entrants in the equipment market when the number of purchasers keeps getting smaller.

This threatens the integrity of our communications networks in the United States—because no network in our globally connected world stands by itself. This means when we think about supply chain security we need to go big and think beyond just our borders. Because despite the FCC's efforts to prohibit equipment that is insecure, domestic networks will still connect to insecure equipment abroad.

So last month at Mobile World Congress I offered an idea for the future. I suggested the FCC should explore opportunities to improve security through open radio access networks—or what is known as open RAN. Instead of relying just on hardware-centric network design offered by a limited number of foreign equipment vendors, we could move to one that is software-

centric. In this new model, we can use off-the shelf hardware and customize through software. This kind of network virtualization flips our traditional way of thinking about equipment supply chains on its head. It pushes the market to where the United States is strongest—in semiconductors and software.

There's been a lot of progress virtualizing network cores. But to date, we have seen less effort to do this in the RAN. Historically it has been the most expensive and restrictive part of the network. In fact today, all major components of a RAN have to come from the same vendor. There is no way to mix and match.

So my idea was to start looking at how we can unlock the RAN and build a more secure 5G future for the supply chain. Because if we can diversify the equipment in this part of our networks, we can increase security and reduce network exposure. It will also mean that carriers in other countries around the world that are locked into upgrade cycles with a single vendor could have a way out. And going forward, it would mean that carriers right here in the United States that are transitioning to more secure equipment could have another path to do so.

But the benefits of an open RAN go beyond security. An open RAN could improve the market for new equipment vendors by lowering barriers to entry. That means more competition and more choice. Moreover, it could help carriers lower their own costs since they no longer have to rip and replace every time there is a network change.

Last month I presented this idea again when I testified before the United States Senate Committee on Homeland Security and Governmental Affairs. It was encouraging because over the course of the hearing, it garnered support from witnesses representing the Department of State, the Department of Commerce, and the Department of Homeland Security.

That doesn't always happen in Washington. So here's what I think the FCC should do next. We should coordinate with other agencies to ensure no single vendor dominates networks. We also should promote more open and interoperable standards for the RAN. The FCC can help by developing testbeds in the United States that bring together operators, vendors, vertical interests, and other government agencies to support these models. We can even build this into our ongoing effort to authorize city-wide 5G testbeds in New York and Salt Lake City. But the primary thing to do is get started—right now.

Second, we need to transform the Internet of Things into the Internet of Secure Things.

You've seen the headlines. The Internet of Things is headed our way in full force. By the end of the decade, globally there will be more than 20 billion connected devices in the world around us. Powered by 5G service, all these connections will provide incredible opportunities to make our lives ore efficient and effective. But as our connections multiply, so do our cyber vulnerabilities.

You can already see it—in efforts to breach city systems, connected cars, and critical infrastructure. The frequency of these events is only going to grow. And while we may be able

to rip and replace the insecure equipment in networks, it would be impractical to think we could rip and replace billions of consumer and industrial Internet of Things devices that connect to our networks.

The reality is that security is no longer as simple as the network you're on because it is dependent on every connection you make at any time. So at the start of this year in a speech at the Center for Strategic and International Studies, I offered an idea to address this challenge. Think of it as a path that can transform the Internet of Things into the Internet of Secure Things.

It goes like this. 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 process for equipment authorization takes place behind the scenes. But why not have the FCC use this equipment authorization process to encourage device manufacturers to build security into new products?

Here's the best part. We could work with the National Institute of Standards and Technology to do it. That's because a few months ago, NIST released a draft set of security recommendations for devices in the Internet of Things. The guide itemizes key cybersecurity features to include in network-capable devices, whether designed for the home, the hospital, or the factory floor. It's thoughtful stuff—like the work NIST does across the board. Plus, it covers so much that is essential—device identification, device configuration, data protection, access to interfaces, and critical software updates.

Once the NIST process is finished, we could use it to update the equipment authorization process at the FCC. In other words, we could update our process to reward those devices that comply, by expediting equipment authorization or expanding our process to include a cybersecurity certification before we offer the FCC stamp of approval on any connected device.

Third—and finally—we need a smarter spectrum policy that supports both security and service in rural communities.

It's important that we do not limit our discussion about security to network equipment. We need to go beyond discussing these problems and get to what is fundamental—and that's spectrum. Because if we want to ensure that we broaden the market for secure equipment we can help the effort along by bringing the right airwaves to market.

On that front, I think the FCC has work to do. Its early efforts to support 5G wireless service have focused on bringing only high-band spectrum—known as millimeter wave—to market. For those keeping track, that's the 24, 28, 37, 39, and 47 GHz bands. These airwaves have significant capacity, but also real propagation challenges. 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 only 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.

This sets us apart from most countries around the world, which are looking to mid-band airwaves for the early 5G wireless deployments. While this spectrum has less capacity than millimeter wave, its signals travel further. That means deployment is more feasible in more places because fewer terrestrial facilities are required to make it work.

Our failure to act early on mid-band spectrum has security consequences. That's because in many of these bands worldwide there is only one Chinese vendor offering equipment. That means countries building their 5G networks now using these airwaves do not have a competitive choice for secure equipment.

In the United States we have unique skill and scale. That means where deployment takes place here, vendors follow. So it's time for us to make it a priority to make mid-band spectrum available, too. There is no reason why our next auction should be a millimeter wave auction. We should be prioritizing the 3.5 GHz band auction and speeding the way for a C-band auction immediately thereafter. If we can do that, our carriers will build there and more vendors will compete to offer service. And when we expand the market for secure equipment at home, it also grows abroad. That's exactly what we need if we want to encourage diversity in open RAN architectures, too. But best of all, it will mean we can extend the promise of secure 5G wireless service to everyone, everywhere in the country.

So there you have it. Three ideas to secure our 5G future. If we get our policies right regarding supply chains, the Internet of Things, and mid-band spectrum we can look forward to a wireless future that is bigger, bolder and safer. It will also be better for rural America. I'm here for that future—and I'm glad you are, too.

Thank you.