STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Report and Order, Further Notice of Proposed Rulemaking (November 22, 2019)

Picture central Montana. It's vast. There are plains as far as the eye can see. This is, after all, Big Sky country. In this wide-open area you'll find mostly wheat and cattle farms. But if you wander you're likely to happen upon Malmstrom Air Force Base. It's the home of the 341st Missile Wing of the Air Force Global Strike Command. On the outskirts of this Air Force Base, you'll find silos with more than 100 intercontinental ballistic missiles. As CNN has reported, they "stand at the ready, buried deep underground." These rockets can deliver nuclear warheads across the ocean thousands of miles away. They are an important part of the United States Strategic Command.

Next to those silos are something a lot more familiar to the Federal Communications Commission. There are clusters of cell phone towers that are operated by a small rural wireless carrier. You might not know it just by looking at them but these towers may represent a bigger risk to our national security than the missiles they surround. That's because the communications equipment that hangs on these towers is from Huawei, and we have good reason to believe it is susceptible to undue foreign influence and control.

Here's the thing. We have long known the risks of deployments that feature equipment developed by vendors like Huawei and ZTE. In fact, the federal government and our four nationwide carriers have shunned this technology because of its security vulnerabilities. But a number of small wireless carriers—serving remote areas like central Montana—have not. After all, Chinese-developed equipment is less costly to deploy and the economics of serving less populated rural communities are hard. So in some cases these insecure networks offer the only option for commercial wireless service in and around sensitive United States military bases in rural parts of the country.

It gets worse. This insecure equipment has been subsidized by the United States government and this very agency. It was purchased with money from the universal service fund at the FCC. If a foreign government ever chose to exploit the radio transmitters that have been placed alongside key military installations, it could suck up sensitive data, shut down service, or launch denial of service attacks. And it gets still worse, because as we transition to next-generation 5G networks, insecure equipment in the telecommunications supply chain could take cybersecurity risks to entirely new levels. That's because 5G networks will allow us to move and access vastly higher quantities of data, and we will depend on them more than prior technologies for a range of mission-critical applications.

This is just one military base in Montana. But there are others like it. Just as there all kinds of essential infrastructure across our rural communities and in many cases nestled nearby are wireless networks with insecure foreign equipment.

We need to do something about it. That's why eighteen months ago we started a rulemaking at the FCC aimed at fixing this problem. Today we take a long overdue first step to do just that. I have only one complaint with this effort: that it took us so long to get here. This is not hard. *It should not have taken us eighteen months to reach the conclusion that federal funds should not be used to purchase equipment that undermines national security.*

I support this effort. I also appreciate that my colleagues were willing to consider changes I offered to the decision and rulemaking we adopt today. In critical part, those include exploring our authority over carriers under the Communications Assistance for Law Enforcement Act to expand our prohibition beyond just the universal service program; providing additional guidance to companies so that our rules do not needlessly disrupt day-to-day service and operations in rural America; implementing the lessons learned from the 600 MHz incentive auction in order to maximize funds available for replacing insecure equipment; and seeking to accelerate the FCC's review of a reimbursement program.

So while I approve today's decision and rulemaking, I think the FCC has more work to do when it comes to network security. Because our present efforts to remove and replace insecure equipment are not bold enough. *We need a coordinated, national plan for managing the future of 5G security—and the evidence all around us makes crystal clear we don't have one.*

When the United States government pursues action against Huawei or ZTE, its objective should be security. But in Washington right now, I fear these issues can easily get swept up into broader trade matters. Despite our actions today, we have to grapple with the fact that at any moment the Administration could trade away our security objectives for some momentary advantage in bilateral trade negotiations. I hope that does not occur, but let's be honest, it has happened before, when this Administration reversed course on banning ZTE from doing business in the United States. If it happens again, it will have serious consequences for our credibility.

There is also a conspicuous lack of progress in other parts of the government tasked with addressing this set of problems. New supply chain rules from the Department of Commerce that were due last month reportedly have been derailed by interagency disputes. The Bureau of Industry and Security has extended three times—and as recently as just this week—the general license authority for United States companies to continue to work with the very companies the FCC is today trying to remove from our networks. On top of this, the national spectrum policy that was announced in last year's Executive Order has fallen by the wayside. It was due in July but is nowhere to be found. And the Administration's tariffs are making it harder for United States companies to invest because by adding up to a 25 percent fee on modems, antennas, and semiconductors it is driving up the cost of 5G deployment.

This does not inspire confidence. It's not a national plan for action. It's the right hand not talking to the left with consequences that are broader than Washington—they go directly to the heart of our competitiveness in the global economy.

Nor has this gone unnoticed. Last week, *The Wall Street Journal* documented all the ways the federal government is tripping over itself in its efforts to support the roll out of 5G. This week, the bipartisan leadership of the Senate Select Committee on Intelligence, Committee

on Homeland Security and Government Affairs, Foreign Relations Committee, and the Armed Services Committee wrote the White House expressing concern that we do not have a coordinated national strategy in place for 5G—and we need one. I agree.

Looking ahead, I have some ideas about just what a national strategy should include. Here are three to start.

First, 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 begin researching how we can build networks that can withstand connection to equipment vulnerabilities around the world. One way to do this is to virtualize and diversify key parts of our networks.

I put forward an idea at Mobile World Congress last month to start this conversation. I suggested the FCC should explore opportunities to support improved security though open radio access networks—or what is known as open RAN. The RAN sits between your device and the core of the carrier network. 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. But if we can unlock the RAN by virtualizing this component of the network with software and off the shelf hardware, we will increase network diversity and improve security at lower cost. Even better, this effort would push the network equipment future to sectors where the United States is strongest—in software and semiconductors.

I offered this idea again when I testified a few weeks ago before the Senate Committee on Homeland Security and Government Affairs. It garnered support from witnesses from the Department of Homeland Security, Department of Commerce, and the Department of Homeland Security. That doesn't always happen in Washington—so we should take advantage of it. Here's what we should do next. The FCC should explore policies to support open RAN and develop testbeds that bring together stakeholders to help promote more open and interoperable standards. We can even build this effort into our ongoing work to authorize city-wide 5G testbeds in New York and Salt Lake City.

Second, we need to transform the Internet of Things into the Internet of Secure Things. With 5G we are moving to a world with billions of connected devices all around us. But as these connected devices multiply, so do our security vulnerabilities. We need to adjust our policies now because the equipment that connects to our networks is just as consequential for security as the equipment that goes into our networks. And while we may be able to rip and replace the insecure equipment in networks, it would be impractical to think we can do the same for billions of consumer and industrial devices in the Internet of Things.

Here is what we can do. Every device that emits radio frequency 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 Institute of Standards and Technology draft set of security recommendations for devices in the Internet of Things. It covers everything from device identification to device configuration to data protection to access to interfaces to critical software updates. In other words, it's a great place to start—and with billions of new devices coming our way we should get going now.

Third and finally, we need smarter spectrum policy. To date, the FCC has 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, and 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 this agency's early 5G efforts will only deepen the digital divide that already plagues too many communities nationwide.

Moreover, our failure to act early on bringing mid-band spectrum to market has security consequences, too. In many mid-band airwaves worldwide there is only one Chinese vendor offering equipment. That means countries building their 5G networks using this spectrum do not have a competitive choice for secure equipment.

In the United States we have unique skill and scale. That means when 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. Instead, we should be clearing the way for the 3.5 GHz band first and following with a C-band auction 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.

Because in the end, that's truly the goal. We want urban America, rural America, and everything in between to know the opportunities of next generation wireless service. But as today's decision and rulemaking make clear—it is not enough just to have access because that access also has to be secure. So if we have vulnerabilities in our networks we need to fix them. If they are in rural areas adjacent to sensitive military installations in Montana or anywhere else across the country we need to replace them. But above all we need to get started. Because this effort represents just that, it has my support.