REMARKS OF
COMMISSIONER JESSICA ROSENWORCEL
"MITIGATING SECURITY RISKS TO EMERGING 5G NETWORKS"
CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES
WASHINGTON, DC
FEBRUARY 6, 2019

Good afternoon. Thank you to the Center for Strategic and International Studies for gathering us here today for a conversation about security and the next generation of wireless technology—known as 5G.

This discussion is timely. Like up to the minute. In fact, when I began to think about how to start my remarks I kept on coming back to the familiar maxim: "May you live in interesting times." Do a little digging online and you will find that there is a dispute about its origin. There is one school of thought that claims it is based on an old Chinese curse. But there is another school that suggests its true provenance lies elsewhere, perhaps with a British statesman. Still, the more that I studied this saying—and the dispute about where it came from—the more that I thought that referencing it was an apt way to begin.

These are interesting times. Last week the Department of Justice charged a Chinese equipment manufacturer and its Chief Financial Officer with attempting to steal trade secrets, obstructing a criminal investigation, and evading economic sanctions on Iran. Last year in the National Defense Authorization Act, Congress prohibited executive branch agencies from using or procuring telecommunications equipment or services from companies that are associated with or believed to be owned or controlled by China. In the meantime, key intelligence allies have joined us in restricting such equipment or are considering ways to do so. Closer to home, at the Federal Communications Commission, we have proposed rules that would prohibit the use of universal service funds to purchase equipment or services from companies "identified as posing a national security risk to communications networks or the communications supply chain."

The stakes are undeniably high. That's because next generation 5G wireless networks are the unifying fabric that will connect us all in the future. This is the essential infrastructure for the next generation of digital technologies. It will feature data speeds 10 to 100 times higher than what we know today with latency reduced to as little as 1 millisecond. This, in turn, will power autonomous vehicles, foster advances in robotics, and expand the potential for machine learning and the possibilities of artificial intelligence.

What this means in practice is that the race to 5G is about so much more than the smartphones in our palms, pockets, and purses. Those handsets represent the epicenter of the last wireless revolution, known as 4G. On its strength we built the applications economy and changed the way we live life online. But the coming changes with 5G are broader. Connecting the physical world around us will change everything from healthcare to entertainment to the way we work and even what work entails. Plus, deploying these networks promises a boost to our economy and millions of new jobs. So it comes as no surprise that countries around the world are jockeying for position and control in this emerging ecosystem. The race to 5G has become a microcosm for the broader debate about global leadership and economic security.

That's heady stuff. To understand it better, I think we would benefit from a bit of communications history. So let's rewind. Let's roll back to some interesting times about two centuries ago. That's when the British Empire dominated global telecommunications through its undersea cable network. It was known as the All-Red line.

The All-Red line has a place in the history books because with such a vast empire, Britain had both the political need for cables to reach far-flung corners of the globe and the expertise to lay them deep on the ocean floor. This tangle of undersea wires stretched from Ireland to Newfoundland, from Singapore to Sydney, and many more places in between. Think of it as the Victorian Internet.

As a result, Britain led when it came to everything involving cable manufacture. It was an expert in cable operation. It dominated the supply of cable building materials. Their engineers were at the forefront of electrical science. So much so, they set the agenda for its research, dictated by the needs of submarine telegraphy.

No wonder, then, that other countries had their submarine cables built, laid, tested, and repaired by British contractors and British ships. In fact, a single British cable manufacturer, TC&M, at one point produced more than half the cables laid worldwide.

For other nations, this leadership had consequences. It meant they were dependent on the courtesies of a foreign government for essential communications facilities, even in times of war.

But the United States wanted to identify other ways forward. We wanted communications systems that were independent. We wanted capabilities in our networks that were less susceptible to foreign control. So what did we do? In time, we invented our way to an expanded market and more secure future.

The spark for this future came in 1901, when Guglielmo Marconi famously sent the first wireless message across the Atlantic Ocean. It wasn't much. But the message—simply the Morse code signal for the letter "s"—traveled more than 2000 miles from England to Canada. But those three clicks of Morse Code were transformative.

The United States took note. It provided a way to communicate with moving ships, blast messages across international borders, and bypass nationally-supported telegraph monopolies. We were all in. The British? They determined this new technology could never challenge their dominance in cable.

Well, we know how this story ends. The All-Red line gave way to a new era of communications. The cable system dominated by the British was supplanted by a more diverse system of interconnected radio networks. In the United States, we saw an inflection point in the development of communications technology and seized it.

Today we are also at an inflection point. What happens with the next generation of wireless services has vast consequences for our economic and national security. The choices we

make now about how these networks are deployed can result in communications technologies that are more powerful by many magnitudes. And getting them deployed early matters. It provides advantages in scale, standards, and device specifications. But I believe it is no longer enough to be first to 5G—the networks we deploy must also be secure. And to build 5G security effectively, we must build a market for more secure 5G equipment. That means making sure our companies can continue to innovate and encouraging other countries to invest in 5G security, too.

This is a big task. As with all significant endeavors, the hard part is where to start. But I have some ideas—about where the FCC should begin.

First, the FCC must work with other agencies to help manage supply chain risk.

Late last year, the Department of Homeland Security announced the creation of the nation's first Information and Communications Technology Supply Chain Risk Management Task Force. This public-private partnership will develop recommendations to identify and manage risk in the global supply chain.

This task force includes representatives from the Department of Homeland Security as well as experts from the Department of Defense, Department of Treasury, General Services Administration, Department of Justice, Department of Commerce, Office of the Director of National Intelligence, and the Social Security Administration. In addition, there is expertise from industry, with representatives from communications carriers, equipment manufacturers, and cybersecurity companies.

It's an impressive list, to be sure. But there's one agency that is missing. The FCC needs a seat at this table. Leaving the agency with primary oversight over communications out is neither prudent nor wise. Moreover, as I mentioned at the start, the FCC has an ongoing proceeding that speaks directly to these issues concerning equipment restrictions on the use of universal service funds.

I believe good things come to those who ask. It is time for the FCC to speak up and secure a commitment from the Department of Homeland Security to participate on this task force. We should be working together. We should develop a common approach to 5G security.

Second, the FCC should charter a new 5G security council.

In past generations of wireless technology, it has been our practice to enjoy their benefits before fully preparing for risk. With 4G and its predecessors, cybersecurity was often an afterthought. It was something to work on when deployment was substantial and when problems revealed themselves through usage. Though the capabilities of these earlier generations of wireless service pale in comparison to those that will emerge with 5G, the vulnerabilities have been real. They range from risks with SS7 networks to rogue use of cell-site simulators. What we have learned is that retrofitting security after the fact is difficult and expensive.

I think we need a more forward-thinking approach to 5G. Cybersecurity needs to be front-of-mind. The good news is that 5G already features many security improvements over

earlier generations of wireless technology. Plus 5G standards are still in early days. Hundreds have yet to be developed. On standards and so much else, there is still front-end work to do.

This is where what is known as the Communications, Security, Reliability, and Interoperability Council comes in. The council is a Federal Advisory Committee that provides recommendations to the FCC on high-profile security-related issues. Its two-year charter comes to an end next month. I think the FCC needs to re-charter and reinvigorate this council. When it does, it should identify 5G security as its focus. To this end, three things need to be a part of its mandate: more study on security technologies to mitigate risk from the Internet of Things, more study on network function virtualization to mitigate denial of service attacks, and a new study on 5G supply chain risk management that recommends specific mitigation techniques.

Third, the FCC needs to make cyber hygiene a priority.

With the advent of 5G services, we will have wireless capability built into the world around us. This will provide a whole new range of opportunities for civic and commercial life. But as they multiply, it will also increase our surface exposure to attack.

To prepare for this future, the FCC will need to expand its work to support cyber hygiene. Think of cyber hygiene this way: To keep our communications systems functioning we are going to need routine practices that increase security and reduce exposure to attack. The agency must build these policies into its day-to-day work.

Consider this: Every device that emits radiofrequency at some point passes through the FCC. Go ahead, take a look at the back of your smartphone, computer, or television. You'll see an identification number from the FCC. That stamp of approval means the device complies with FCC rules and policy objectives before it is marketed or imported into the United States.

Now picture this: Going forward the number of devices could expand exponentially with 5G and the Internet of Things. So what if the FCC used its equipment authorization process to encourage device manufacturers to build security into new products? To this end, it could seek a disclosure from manufacturers that explain how new devices are secure throughout the expected lifecycle of the equipment. This would support better security practices on the millions of devices headed for us with the Internet of Things.

Or consider that telecommunications carriers are required to certify annually that they comply with FCC privacy standards. There is, however, no equivalent agency certification required for security. What if we changed that? What if with the next generation of wireless licenses we ask that as a condition of holding a public license, licensees certify that they have implemented the best practices for 5G security? For example, we could ask that licensees certify that they are using the National Institute of Standards of Technology Cybersecurity Framework. That way, we can ensure that licensees have a structured way of thinking about network security and are using a common language for managing risk.

Finally, the FCC should take steps to educate citizens about cyber hygiene. In our work, we regularly interact with consumers and consumer groups. We need to find more ways to do

outreach that touch on the basics of cyber hygiene—from downloading software upgrades for devices to assessing connection security when using unlicensed airwaves.

Those are my ideas for getting this conversation started. These are early days in the deployment of 5G. As I said at the start, they are interesting times. It is also the right time to ensure that communications security is front and center.

Thank you.