REMARKS OF
ACTING CHAIRWOMAN JESSICA ROSENWORCEL
"ACCELERATING 5G IN THE UNITED STATES"
CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES
WASHINGTON, DC
MARCH 18, 2021

Good morning! Thank you to the Center for Strategic and International Studies for convening this discussion and inviting me to participate. Thank you also for your working group's new report on 5G security. It's full of keen analysis and smart recommendations—and I'm not just saying that because it echoes a lot of our work at the Federal Communications Commission. It's also treat to be here with Congresswoman Matsui—especially in a setting where I'm not being cross-examined by the Energy and Commerce Committee. She is a true thought leader on Capitol Hill, especially when it comes to spectrum policy.

This is actually my second time speaking to CSIS. You hosted me back in early 2019. I opened those remarks by noting how timely it was to be holding a discussion about the security of our communications networks. Just days earlier, the Department of Justice had charged a Chinese equipment manufacturer and its Chief Financial Officer with attempting to steal trade secrets. Back then the presence of network equipment from untrusted Chinese vendors was viewed as one of the greatest cybersecurity challenges facing the country.

Then my predecessor at the FCC spoke to CSIS in early 2021. That took place two weeks after news broke about the SolarWinds breach, which allowed hackers to penetrate the Pentagon, nuclear labs, the State Department, the Department of Homeland Security, and other offices that used the company's network-monitoring software. It has been described as the biggest and most sophisticated hack the world has ever seen.

Now I find myself speaking to CSIS again, on the heels of yet another major cybersecurity story. Last week, Microsoft revealed that security for its Exchange software had been breached, leaving hundreds of banks, healthcare, and government servers vulnerable to hackers.

So it's safe to say, we've reached a point where we are never that far removed from a new development to remind us that, when it comes to cybersecurity, the threats are real, the stakes are high, and our defenses may be insufficient. In other words, we live in an age where talk of cybersecurity and how to improve it is *always* a timely discussion.

What strikes me is that each of these events unfolded like a scene from a scary movie: we frantically barricaded the doors, only to discover that the threat had been hiding inside the whole time. For years while we sought to protect ourselves from external threats, untrusted equipment and services had been sitting undisturbed in our nation's commercial networks.

Now let me pause here and make something of a confession. I'm that person that talks back at the television screen. I'm sure I'm not the only one. Some people jump, some people

close their eyes—I've got ideas about what ill-fated characters could be doing to better their fate, and an unabashed proclivity toward sharing them.

So today I'm not going to hold that tendency back. I'm going to share three lessons we've all learned from these movies that should apply equally to our nation's cybersecurity.

Of course, I want to start by recognizing that the cybersecurity challenge is about to get even more challenging with the advent of 5G.

That's because our 5G future is about connecting everything. It is about moving to a new networked world that will open up possibilities for communications that we cannot even fully imagine today. By exponentially increasing the connections between people and things around us, this technology could become an input in everything we do—improving agriculture, education, healthcare, energy, transportation, and more. The data we derive from all these connections is powerful—it will inform machine learning, artificial intelligence, and the next generation of innovation across the economy.

But building this future right means building security in front from the start. That's because this new endless connectivity also means new vulnerabilities. With so much on the line, it's urgent that trustworthy companies build the next-generation networks that will soon touch so much of our lives. And it's critical that we take a multifaceted and strategic approach to protecting our networks from all threats.

So let's get started.

Lesson One: Never Split Up.

It's a terrible idea for horror movies and it's a terrible idea for cybersecurity too. There is no task at the FCC—or in any part of the federal government—that is more important than keeping the American people safe. But history demonstrates that no single entity can meet this challenge alone. That is why in my first meeting as Acting Chairwoman I committed to working with our federal partners and the private sector to increase the security and resiliency of our nation's communications networks. I also made clear my belief that working with like-minded countries and multilateral institutions and building on shared frameworks like the Prague Principles can multiply our strength across the globe.

This is more than just rhetoric. In my first few weeks as Acting Chairwoman I made it a priority to reach out to my peers in other parts of the federal government to help coordinate and advance our shared interest in network security. Those efforts included speaking with present leadership at the National Telecommunications and Information Administration, the Cybersecurity and Infrastructure Security Agency, and the Deputy National Security Advisor for Cyber and Emerging Technology in the new Administration.

And while we make it a priority to coordinate externally—whether with other countries or other agencies—we need to do the same internally. So I have updated the way that the FCC reviews matters related to national security, which right now are siloed within the agency's

various bureaus and offices. If we are going to keep pace with the growing threats to our communications, we need a dedicated interagency and cross-bureau team of experts advancing a comprehensive approach to securing our nation's communications.

This team is already hard at work. That includes auditing and updating the FCC's capabilities on national security issues, exploring opportunities to collaborate with other federal agencies—like the National Science Foundation and the Department of Defense—on new 5G testbeds, rechartering and rejuvenating the FCC's Communications Security, Reliability, and Interoperability Council for our 5G future, and addressing evolving national security risks in this agency's past grants of Section 214 applications. We expect to have more to announce on each of these fronts soon.

So that's lesson one. Let's keep going.

Lesson Two: Don't Answer the Door.

Or to put it somewhat differently, don't let the threat inside your home.

When it comes to a 5G security strategy, the government's approach to date has focused on slowing down untrusted vendors. We know there are risks that come with using this equipment and those vulnerabilities could provide foreign interests with access to our networks, jeopardizing the security of communications in the United States. So we've rolled out policies aimed at slowing down the adoption of Huawei and ZTE equipment globally, targeting these companies' practices that allow them to move quickly, and leveling the international playing field.

At the FCC we restricted the use of this equipment by carriers through changes to our universal service fund. Thanks to the Secure and Trusted Communications Networks Act, we are putting the finishing touches on a system to replace insecure equipment from Chinese companies like Huawei and ZTE, to the extent that it is present in our domestic networks today. Congress has appropriated $1.9 billion for the FCC to do this work. And in February, at my first meeting as Acting Chairwoman, the Commission launched a proceeding to get that money out the door and get going on this important work.

We're broadening our focus from equipment to services too. We previously denied an application from China Mobile USA to enter our markets and put four other similarly situated companies on notice they could share a similar fate. Yesterday we instituted proceedings to revoke the domestic authority and international authorizations of three of those companies: China Unicom Americas, Pacific Networks, and ComNet.

Finally, we're increasing transparency and information sharing around these issues, too. The Secure and Trusted Communications Networks Act requires that the Commission publish and maintain a list of communications equipment and services that pose an unacceptable risk to national security or the security and safety of U.S. persons. Just last week, our Public Safety and Homeland Security Bureau released its list of unsafe vendors, which includes Huawei, ZTE and three other Chinese companies identified by Congress. As we continue to update and maintain

this list, it will provide meaningful guidance that will ensure that as next-generation networks are built across the country, they do not repeat the mistakes of the past.

Collectively, I believe these actions will help make our communications future more secure. If we do these things right, we have an opportunity to serve as a model for the rest of the world on how to remove insecure equipment and services from communications networks. We have the funding, the congressional mandate, the ears of policymakers, and the eyes of the world. So let's make the most of this moment.

And that brings us the end.

Lesson Three: Have a Back-Up Plan.

It's just common sense.

Now I said earlier that the FCC's focus to date has been on slowing down untrusted vendors. But I believe there is another strategy that we should be pursuing at the same time. While we continue to take action to slow down untrusted vendors, *we also must take action to speed up American innovation*.

So to get that effort started, yesterday the agency launched the first-ever inquiry into open radio access networks—or open RAN.

This is important because we have only four major vendors for RAN equipment to choose from, none of which hails from the United States. Plus, the vendors that have grown fastest in recent years are from China, in part because the Chinese government deploys powerful industrial policies to make their equipment cheaper to deploy than the alternatives. We know based on a comprehensive record developed by various national security agencies around the world that there are serious risks that come with having this equipment in our networks.

On top of that, the RAN is the most restrictive and most expensive part of the network, in part because all of its major components have to come from the same vendor. There is no way to mix and match.

So here's the thinking behind open RAN. If we can unlock the RAN and diversify the equipment in this part of our networks, we may be able to increase security, reduce our exposure to any single foreign vendor, lower costs, and push the equipment market to where the United States is uniquely skilled—in software.

That sounds promising. And as a result of our action yesterday, we will have the first comprehensive record on the public interest benefits of new interoperability in the RAN. We will have the first assessment of the state of this technology, how our rules may be adjusted to foster its growth, and how our coordination with other federal actors—from the National Science Foundation to the Department of Defense—may stimulate its development in the marketplace.

At the same time, we do not shy away from the hard questions. We ask about challenges associated with systems integration and management. We consider reliability and quality of service. We ask whether new openness also could introduce new vulnerabilities to the network. These questions are important to understand whether open RAN will deliver on its national security promise.

Of course, our network equipment is only as good as the spectrum it runs on. So we are not slowing down there either. Yesterday the FCC took decisive action to pivot to mid-band for 5G. We did that by adopting rules and auction procedures that will make 100 megahertz of prime mid-band spectrum in the 3.45-3.55 GHz band available for 5G this year. And we are tying this new spectrum to the most aggressive build-out obligations of any spectrum auctioned for 5G to date.

This decision offers tremendous opportunity because during the past few years the United States was slow, relative to other countries, to recognize the importance of mid-band spectrum for 5G. This meant we were late to bring these airwaves to market. So mid-band spectrum has been the critical component that is missing, and our action here helps fix that.

This is all progress we can be proud of. No talking back to the screen required. But we need to continue to talk about network security and the roll-out of 5G service at home and abroad. The opportunities for innovation are extraordinary. But the vulnerabilities this connectivity brings deserves attention—and I'm glad that CSIS is here to provide a forum for discussion. Because it's important for the United States to get this right. In fact, it is essential for our 5G leadership in a post-pandemic world.

Thank you.