REMARKS OF
ACTING CHAIRWOMAN JESSICA ROSENWORCEL
TO THE COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL
SEPTEMBER 22, 2021

Welcome to the inaugural meeting of CSRIC VIII. I appreciate your willingness to bring your time and talents to this Council. I know that together you will provide us with incredibly valuable perspective as we sort through some of the toughest security problems facing our country's communications networks. The issues before you may not always have easy answers, but I believe the breadth of experience represented by this Council's membership is exactly what we need to tackle this challenge and find a way forward.

This is my first time speaking to CSRIC as Acting Chairwoman. But it's not the first time I've spoken about the issues you have been brought together to address. Lately, I've made a habit of starting my speeches about network security by recounting the latest breach that caught the nation's imagination. So when I spoke at the FCC's Supply Chain Integrity Workshop back in April, I talked about how KPN, one of the Netherlands' largest wireless carriers, discovered that the calls of 6.5 million subscribers—including the Dutch Prime Minister—may have been susceptible to monitoring because of insecure equipment in their networks.

Before that, at the Center for Strategic and International Studies, I started with the news that security for Exchange software had been breached, leaving a wide swath of bank, healthcare, and government servers vulnerable to hackers.

Just two months before that, I spoke about the SolarWinds breach, which allowed hackers affiliated with the Russian government to roam about government and private networks for months undetected.

I could go on because the streak continues. Just yesterday, the *Washington Post* reported a ransomware attack on an Iowa farming co-op. And last month, a hacker stole data on more than 50 million customers from a nationwide wireless carrier.

The truth is that every day in our connected digital life there are too many cyber events that have the potential to harm the safety and well-being of people and businesses across the country. And no entity is immune from this threat—whether large or small, public or private, prepared or unprepared.

I know we are all thinking it, so let me say it out loud: this needs our attention because enough is enough.

Well, I think it's time to turn that resolve into action. Because when it comes to network security, the threats are real, the stakes are high, and our defenses need to evolve and improve. This is especially vital as we transition to next generation 5G networks that will connect so much more in the world around us. I know that when we deploy this technology extraordinary opportunities will follow, but only if we properly secure our networks and the communications supply chain.

That's why at the FCC we are pursuing a proactive, three-pronged strategy to help build a 5G future that is secure. There's a lot of work on that already underway. We are taking direct action to keep untrusted vendors out of our communications networks, where they can do real harm—thanks in part to the Secure and Trusted Communications Networks Act. We are speeding up trustworthy innovation so that we can develop a market for secure 5G equipment alternatives like Open RAN. And we are collaborating across government, with industry, and with partner nations on a multifaceted, strategic approach to protect our networks from all threats.

That's where you come in. In this environment, rechartering CSRIC was a no-brainer. This Council is one of the nation's most impactful cybersecurity partnerships. But we didn't want to do it same-old, same-old. We wanted to make it better. We wanted to make sure this CSRIC was made for the moment and well-positioned to accomplish its mission. So we've made some notable improvements.

Let's start with the big news. For the first time ever, CSRIC VIII will be co-chaired by the Cybersecurity and Infrastructure Security Agency—or as most of us know it—CISA. This is really important. CISA leads the coordinated national effort to enhance the security, resiliency, and reliability of our cybersecurity and communications infrastructure. And earlier this year, CISA co-authored a leading report on potential threat vectors to 5G infrastructure. Their partnership here will help ensure a unity of effort between those responsible for protecting the country and those who own and operate the infrastructure that is so critical to that mission. I'm thankful for CISA for working with us to make this happen.

In addition, CSRIC VIII will reflect more participation from the public interest community. This means that the public and consumers also will have a voice on issues that ultimately affect their safety and security along with private sector stakeholders.

On top of that, we gave CSRIC VIII a fresh agenda with a 5G focus. That means we have a working group to explore the security and resiliency of Open RAN. We have a working group looking at more broadly leveraging virtualization technology to enhance network security. We have a working group looking at the technical issues involving the security of 5G signaling protocols. And building on CSRIC's earlier work to remove untrusted hardware from our communications and infrastructure and building on lessons learned from the SolarWinds hack, we have a working group looking at the software side of supply chain security.

But as they say—that's not all. Earlier this month, Hurricane Ida knocked cell sites offline in the hardest hit parts of Louisiana. So we are making sure that CSRIC VIII makes progress on the resiliency of our communications networks, too. We've got a working group to look at improving 911—specifically 911 service over Wi-Fi. And we have yet another working group that will be looking at ways to improve Wireless Emergency Alerts.

It's a lot—and I'm excited about the work you'll do on all these issues. Think of it as a to-do list of security challenges that we already know about. But it's not enough to just keep your heads down and do the work before you. Because I want the experts in this audience to keep your eyes up and be on the look-out for threats that are just around the bend. These issues

are evolving fast and it can often feel like we are playing catch-up. So I'm calling on all of you to use your imagination and expertise to help us stay one step ahead of those who would do us harm.

I know this is a tall task. But looking at the talent we've assembled, I know you're up to it. Thanks again for your service to this Council and our country. Now let's get to work.