REMARKS OF
ACTING CHAIRWOMAN JESSICA ROSENWORCEL
FEDERAL COMMUNICATIONS COMMISSION
SUPPLY CHAIN INTEGRITY WORKSHOP
APRIL 26, 2021

Good morning and happy Monday. Hopefully, you've all had a relaxing and restorative weekend—and some coffee, too—because we are going to start this week at the FCC with in-depth dialogue about network security. We're cosponsoring this event with the Office of the Director of National Intelligence, and we're holding it during National Supply Chain Integrity Month, which is a call to action for organizations across the country to strengthen their supply chains and also protect them foreign risk. Of course, doing so is a government-wide effort. So a special thank you is in order to our other federal partners who are also joining us. You'll hear from the NTIA and others at the Department of Commerce; the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency; the General Services Administration; and the FBI.

Most of all, thank you to everyone at the FCC who has been working on this event and these issues. I'm pleased to say that all four of my fellow Commissioners have agreed to join us today. I know that each of my colleagues has a deep interest in the subject at hand and a strong commitment to tackling supply chain security. I know they would also agree that the people who really deserve praise are our outstanding FCC staff. If it weren't for them, we wouldn't have this all-star lineup for this workshop, and I wouldn't have a list of accomplishments to tout in my remarks. Leading the way on this work is our Public Safety and Homeland Security Bureau. You already heard from the Bureau's Deputy Director, Debra Jordan, and to close out today's workshop you'll hear from the Bureau's Chief, Lisa Fowlkes. They've got a great team, and they've put together a great event. Thanks also to our other Bureaus and Offices for their contributions today. Just as network security requires collaboration across multiple government agencies, this is an all-hands effort at the FCC, too.

As a nation, some of the newest threats we face, and perhaps some of the fastest growing, are those in our communications supply chains. The last time I gave a speech on network security was about a month ago at the Center for Strategic and International Studies. A week before I delivered those remarks, Microsoft revealed that security for its Exchange software had been breached, leaving a wide swath of bank, healthcare, and government servers vulnerable to hackers. When my predecessor at the FCC spoke to the same organization about network security just two months before, news had broken out about the SolarWinds breach, which allowed hackers affiliated with the Russian government to roam about government and private networks for months, undetected.

Suffice it to say, we've reached a point where we are never that far removed from new reports of a security breach. So right on cue, we have a story out of the Netherlands last week. A Dutch newspaper reported that a decade ago, KPN, one of the Netherlands' largest wireless carriers, hired a third party to assess the security risks created by their decision to start using Huawei equipment in their communications networks. Notably, this audit came at the urging of Dutch security services. The recently revealed report concluded that there were real security flaws in the network, which could have made the calls of all 6.5 million KPN subscribers, including the Dutch Prime Minister, susceptible to monitoring. Faced with these reports, Huawei has denied any wrongdoing. But, I would note that KPN was one of the first European operators to reverse course and exclude the company from its core 5G network.

These stories are multiplying. For that reason, there can no longer be any question that, when it comes to network security, the threats are real, the stakes are high, and our defenses need to constantly 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 these networks extraordinary opportunities will follow, but only if we properly secure our communications supply chain.

At the FCC, under my leadership, we are pursuing a proactive, three-pronged strategy to building a more secure, resilient, and next-generation communications supply chain for this 5G future. To start, we are taking direct action to slow down untrusted vendors both at home and abroad. But we are also recognizing that "Just Say No" is not a strategy. So we are moving fast to speed the way for trustworthy innovation. Finally, we are collaborating across government, with industry, and with partner nations on a multifaceted, strategic approach to protect our networks from all threats.

First—Slowing Down Untrusted Vendors. At the FCC we're making significant progress keeping untrusted equipment out of our networks. We've prohibited the use of federal funds from the agency's universal service program to purchase equipment that could pose a national security threat to the United States. Thanks to the Secure and Trusted Communications Networks Act and a $1.9 billion appropriation from Congress, we now are putting the finishing touches on a program to replace this equipment to the extent that it is present in our domestic networks today.

We are increasing transparency and information sharing around these issues, too. Last month, we published a first-of-its kind list of communications equipment and services that pose an unacceptable risk to national security. Going forward, we are working with other federal agencies to maintain this list and ensure that it is providing the private sector with the most up-to-date information they need to make the right decisions about security. We are also exploring additional consequences for companies on this list—including what it means for their participation in other programs like the United States' equipment authorization regime.

Finally, we're broadening our focus beyond equipment to services, too. We previously denied an application from China Mobile USA to enter our markets after finding that the company is ultimately owned and controlled by the Chinese government, and we recently put four similarly situated companies on notice that they could share a similar fate. I also have directed the FCC's International Bureau to look back at this agency's past grants of international applications and recommend options for addressing evolving national security risks.

Second—Speeding Up Trustworthy Innovation. While we continue to take action to slow down untrusted vendors, I believe we also need to take action to speed the way for trustworthy innovation, too.

To get this effort started, last month I launched the first-ever inquiry in the United States into open radio access networks, or open RAN. There is good reason to think that disaggregating the RAN brings real benefits for the supply chain, including more security, lower costs, more competition, and reduced exposure to any single foreign vendor. It could also push the network equipment market to where the United States is uniquely skilled—in software. In light of this proceeding, we will have the first broad-based assessment of the state of this technology, how our rules may be adjusted to foster its growth, and how our coordination with federal actors—from the National Science Foundation to the Department of Defense—could stimulate its development in the marketplace.

Third—Collaborating with Government, Industry, and Partner Nations. When it comes to supply chain security, we know that no single entity can meet this challenge alone.

That is why in my first few weeks as Acting Chairwoman I made it a priority to coordinate with my peers in other parts of the federal government to advance our shared interest in network security. Those efforts included speaking with present leadership at the NTIA, the Cybersecurity and Infrastructure Security Agency, and the Deputy National Security Advisor for Cyber and Emerging Technology.

I also updated the way the FCC reviews matters related to national security with the creation of a special team of experts from across the agency charged with advancing a comprehensive approach to securing our nation's communications, which we are calling the FCC's National Security Policy Council.

I am also leveraging the technical know-how and execution prowess of industry. Earlier this month, I announced that we will be re-establishing the FCC's Communications Security, Reliability, and Interoperability Council and giving it a 5G focus. In addition, following security breaches that have impacted the communications sector, we will ask the CSRIC to review risks to service provider operations from attacks in software and cloud service stacks and to develop mitigation strategies.

Finally, I am embracing work with our partner nations, too. Just this month, I had the privilege of signing a Memorandum of Understanding with the Chair of the Independent Communications Authority of South Africa—our first MOU with a sub-Saharan African nation in decades—and we are working hard to build trust and expand these kinds of partnerships across the globe.

So that is a quick summary of what we're doing to date. Stay tuned because more is coming ahead. Now let me close with a request. I appreciate a thoughtful discussion on supply chain security. But what I'm really interested in is action and results. So let's commit to making sure that the ideas that we share and the connections we make today will drive tangible action to improve network security. I'm here for it—and I know my colleagues are, too.

Thank you again for participating in this event. Now let's get to work.