REMARKS BY FCC CHAIRMAN AJIT PAI
TO THE PRAGUE 5G SECURITY CONFERENCE

SEPTEMBER 24, 2020

Thank you, Jakob, for that introduction. And thanks to Prime Minister Andrej Babis and everyone at the Czech National Cyber and Information Security Agency and the Ministry of Foreign Affairs for hosting this conference and inviting me to participate. It's become clichéd to say on videoconferences that I regret that we aren't meeting in person, but I *really* mean it this time because a virtual discussion means that I can't return to Prague. But in all seriousness, whether in person or online, it's an honor to join my colleagues from Australia, France, the Netherlands, and the European Union on this panel.

The fact that we are together today means a few things. One, it means last year's Prague 5G Security Conference was a success. After all, they don't make sequels for movies that flop. Second, it means 5G security is still a pressing issue and we still have work to do.

Not long from now, 5G networks will be embedded in almost every aspect of our society and economy—from homes to businesses, hospitals to transportation networks, manufacturing to the power grid. In other words, the number of cybersecurity attack vectors are about to grow exponentially.

We've gathered to discuss 5G security, of course, but I think it's important to say up front that we can't let these challenges hold back our efforts to unlock the possibilities of 5G itself. Over the past few years, the FCC has aggressively executed what we call our 5G FAST plan. This strategy for promoting 5G innovation and investment features three key parts: freeing up commercial spectrum, promoting the installation of wireless infrastructure, and encouraging fiber deployment.

This strategy has yielded significant results. For example, we've completed four auctions in less than two years that have repurposed massive amounts of spectrum for 5G. In addition, we continue to modernize regulations and promote infrastructure build-out. This has spurred record-breaking capital investments in infrastructure essential for 5G, including fiber-optic cables and small cells.

But as important as our 5G FAST plan is to facilitating 5G network deployment, these gains can be severely undermined if we can't ensure that these networks are secure.

For the United States, addressing the national security threats posed by certain foreign communications equipment providers is a whole-of-government effort. Earlier in this conference, you heard from U.S. Secretary of State Mike Pompeo about the various initiatives across the U.S. Government to secure our nation's critical information and communications infrastructure. This includes the Department of State's Clean Path Initiative, which requires all 5G network traffic entering and exiting U.S. diplomatic facilities to connect using network equipment from trusted vendors. And you heard from Deputy Assistant to the President for Cyber, Josh Steinman, about the broad-ranging National Strategy to Secure 5G signed by President Trump in March. This reflects the U.S. Government's multifaceted approach to 5G supply chain security, and it highlights the need for close collaboration with international partners and industry to advance 5G security and promote 5G vendor diversity.

At the FCC, we are doing our own part to promote 5G security. At last year's conference, I gave an overview of the FCC's actions. Much has happened since then.

As the telecommunications regulator for the United States, our focus has been on protecting the security and integrity of the communications supply chain.

Specifically, since the first Prague 5G Security Conference, the FCC has prohibited the use of money from our Universal Service Fund, or USF, to purchase or obtain any equipment or services produced or provided by companies that the Commission determines pose a national security threat. And we specifically designated Huawei and ZTE as companies that pose a national security threat.

We also started a process to identify and catalog insecure equipment used in USF-funded communications networks so we can work to implement a program to remove and replace it. We recently completed this review and released our findings earlier this month. We determined that it could cost at least $1.837 billion to remove and replace Huawei and ZTE equipment in U.S. networks. We are working with the U.S. Congress to secure the necessary funding to do just that.

At last year's conference, I noted that the FCC was poised to deny China Mobile's application to enter the U.S. market. We did, in fact, reject that application in May 2019. This decision came after a lengthy review of the application by Executive Branch agencies and consultation with the U.S. intelligence community. We concluded that China Mobile's application posed substantial national security and law enforcement concerns that could not be adequately mitigated.

Following our decision to deny China Mobile's application, we have issued orders to four other Chinese state-owned companies—China Telecom, China Unicom, Pacific Networks, and ComNet—that already hold such FCC authorizations. The orders require these companies to demonstrate why the FCC should not revoke and terminate their authorizations to operate in the United States based on similar national security concerns.

These regulatory steps are critical to protect the integrity of our 5G networks. But they are not the only forces at play. Companies building 5G networks have an economic incentive to address security concerns and to find alternatives to untrusted vendors.

Many carriers building out 5G networks are recognizing that you get what you pay for, and that the long-term costs of using insecure equipment are likely to outweigh any short-term savings. Making the right choices early on in the network planning and deployment process is much easier and ultimately cheaper than trying to correct mistakes once network construction and operation is well underway, as evidenced by the FCC's recent survey that came up with the $1.8 billion price tag to remove and replace risky equipment in U.S. networks.

Unfortunately, much of the equipment at the heart of 5G networks currently comes from just a few global suppliers, with Huawei being the largest. This lack of vendor diversity can make it challenging for some carriers to find cost-effective alternatives. However, technological innovation has provided a new path to address these concerns. As mentioned on a previous panel, Open Radio Access Networks, or Open RANs, could transform 5G network architecture, costs, and security.

Just a few weeks ago, the FCC held a forum on 5G open, interoperable, standards-based, and virtualized radio access networks. It featured top experts from the United States and around the world to encourage research and development of these systems, which can enable a diversity in suppliers, improve network security, and lower costs. A consensus emerged from the forum that Open RAN technologies are already showing great promise in the U.S. and around the world, and that the public and private sectors should continue to collaborate to help encourage their deployment.

As we have pursued our own actions to address security threats, the United States has been working closely with our international partners. As the very fact of this conference highlights, international cooperation is critical if we are to protect our 5G infrastructure.

Since we met in Prague in May 2019, there has been substantial progress in adoption of policies to secure 5G networks, as outlined in the Prague Principles, including the July 2020 announcement by the United Kingdom that it will remove Huawei equipment from its 5G networks. The United Kingdom decision comes as a number of countries across Europe—including the Czech Republic, Poland, Romania, Denmark, Estonia, Latvia, Sweden, and Greece—have taken steps prohibiting these high-risk vendors from their networks. And we observe how telecommunications operators are also taking actions to make their networks secure. Telefonica in Spain, Orange in France, Jio in India, Telstra in Australia, SK and KT in South Korea, NTT in Japan, and the telecom operators in Canada and Singapore, as well as many others, have made the decision to only use trusted vendors in their 5G deployments.

And as I engage with other communications regulators around the world, the Prague Principles have been an important part of our discussions about protecting 5G networks.

I look forward to continuing our engagement with all of you on these issues and to advancing the Prague Principles, and now the Prague 5G Repository, around the world as part of that engagement. As so many have mentioned over the course of our discussions here, efforts to secure 5G networks do not stop at our borders. We are in this together.