REMARKS OF CHAIRMAN AJIT PAI
AT THE PRAGUE 5G SECURITY CONFERENCE

PRAGUE, CZECH REPUBLIC

May 2, 2019

Before we begin, I would like to start by saying děkuji—thank you—to Minister Petříček and everyone at the Czech Ministry of Foreign Affairs for hosting this conference and for inviting me to participate and moderate this session. I also want to thank and recognize Prime Minister Andrej Babis for convening this conference and for taking the time to personally participate in the opening session.

This is my second 5G event in the past three weeks that featured a head of government.

In mid-April, I was at the White House with President Trump to highlight American efforts to promote the development and deployment of 5G technologies.

When Presidents and Prime Ministers get personally involved in a communications issue, the message is clear: 5G is a critical subject with major implications for economic growth, national security, and our quality of life.

5G networks will be much faster and carry much more data. In time, they will bring applications and services we can't even imagine today. But we've come together this week to focus on another important issue: how we can make sure these networks are safe and secure.

The fact that dozens of nations are represented here shows that there is a broad consensus that network security is not only a priority but a necessity for 5G. Indeed, going forward, 5G network security will impact our respective countries' national security.

I look forward to hearing on this panel private-sector perspectives from AT&T, Orange, Deutsche Telekom, and Vodafone on the development and deployment of secure 5G networks.

Their input matters because of the central role that industry is playing and will continue to play in 5G. For example, as President Trump put it at the April event, "In the United States, our approach is private-sector driven and private-sector led."

For that reason, we at the FCC are implementing our 5G FAST plan—a plan to expedite private-sector 5G deployment, and one which consists of three key parts.

First, we're freeing up spectrum. We recently finished an auction of spectrum in the 28 GHz band in January. We are currently conducting an auction of the 24 GHz band. And we recently announced that, on December 10, we'll be launching a single auction of 3,400 MHz of spectrum in the 37, 39, and 47 GHz bands. We've also been working to repurpose mid-band spectrum for 5G. Among other steps, we will be holding an auction in the 3.5 GHz band next year.

Second, we're making it easier to install small cells and other wireless infrastructure, which will be key to densified 5G networks. We set a reasonable deadline for cities to rule on siting applications and reasonable limits on siting fees. We also eliminated rules to make sure that infrastructure the size of a pizza box won't face the same regulatory review as a 60-meter tower.

Third, we've modernized our rules to encourage the deployment of optical fiber for backhaul. We've done a lot to make that happen, from ending heavy-handed utility-style regulations to making it easier and cheaper for companies to attach fiber to utility poles.

The FCC's 5G FAST plan is already getting results in terms of private investment and deployment in 5G. But what are we doing about network security—the central theme of this gathering?

In the United States, many agencies have important responsibilities when it comes to ensuring the safety of our networks. And at the FCC, we are playing our part. One of our top priorities must be protecting the security and integrity of the supply chain. That's why the FCC has proposed to prohibit the use of the broadband funding we administer to purchase equipment or services from any company that poses a national security threat to the integrity of United States communications networks or the communications supply chain.

In addition, the FCC will vote next week to reject China Mobile's petition to provide international telecommunications services in the United States. This decision comes after a lengthy Executive Branch review of the application and consultation with the U.S. intelligence community, which concluded China Mobile posed substantial national security and law enforcement concerns that could not be adequately mitigated.

Stepping back and looking at the bigger picture, we believe that 5G security issues need to be addressed upfront. Making the right choices when deployment is beginning is much easier than trying to correct mistakes once network construction and operation is well underway. Moreover, decisions that impact 5G security need to be made with the long term in mind. Focusing too heavily on short-term considerations could result in choices that are pennywise but pound foolish.

Similarly, when making decisions that impact 5G security, we need to remember that its implications are wide-ranging. 5G will have a transformational impact. It will affect our militaries, our industries, our critical infrastructure (from ports to electric grids), our entrepreneurs, and much more. The procurement and deployment decisions made now will have a generational impact on our security, economy, and society.

In the international realm, too, security cooperation will depend in part on secure 5G networks. I will put it plainly: when it comes to 5G, we cannot afford to make risky choices and just hope for the best. We must see clearly the threats to the security of our networks and act to address them. And the more that the nations represented at this conference can work together and make security decisions based on shared principles, the safer that our 5G networks will be.

Thank you once again to our hosts for convening this conference. The United States stands ready and willing to work with all of you on this important issue. And now, we will hear perspectives on deployment and security from those in the private sector who are building the 5G future.