OPENING REMARKS OF COMMISSIONER BRENDAN CARR

WASHINGTON FOREIGN PRESS CENTER

"ENSURING THE SECURITY OF 5G NETWORKS"

WASHINGTON, D.C.

NOVEMBER 26, 2019

Thank you to the U.S. Department of State for the invitation to participate in this press briefing. I look forward to discussing 5G and the steps we're taking in America to ensure secure, trusted, and vibrant communications networks around the globe. I am happy to take questions from the esteemed members of the foreign press that are here today. And I would like to begin by offering some brief opening remarks.

Advancing the buildout of 5G networks has been a leading focus for me at the Federal Communications Commission. After all, 5G networks will be the platforms upon which a new wave of jobs and economic opportunity will be created. Indeed, all of the life-changing technologies we hear about—from autonomous cars to smart cities, from remote surgery to virtual reality—won't work or won't work well without 5G.

As networks transition from carrying voice calls and emails to these life changing applications, the security of those networks becomes only more important. There's already so much in modern society that now runs on interconnected networks, from banking, to transportation, and even our power grids. This will become only more so as carriers continue to build out 5G networks. If these networks are threatened, everything we have come to rely on is threatened.

In the U.S., we have acknowledged the threat that Chinese telecom firms pose to our networks for some time. In 2012, the House Permanent Select Committee on Intelligence issued a report recommending that companies avoid using Huawei and ZTE equipment. In 2018, Congress passed the National Defense Authorization Act, which prohibits U.S. government agencies and contractors from using Chinese equipment. In May of this year, President Trump issued an Executive Order to secure our ICT infrastructure and supply chains. Separately, the U.S. Department of Commerce added Huawei to the Entity List, which imposes restrictions on its access to U.S. markets, based on a determination that the company engaged in activities that are contrary to U.S. national security interests. And just this month, U.S. Attorney General William P. Barr filed a letter at the FCC stating that "we should not signal that Huawei and ZTE are anything other than a threat to our collective security."

The FCC opened a proceeding on the threats posed by Huawei, ZTE, and other equipment providers last year. The record that developed made clear the security threats posed by these firms. Both companies have close ties to China's Communist government and military apparatus. It's been reported, for instance, that Huawei employees work as agents for the People's Liberation Army. Both companies are subject to Chinese law that obligates them to cooperate with any request from the country's intelligence services and to keep those requests secret. Indeed, China's National Intelligence Law requires that all "organizations…cooperate with the State intelligence work," and it provides them no right to refuse. It also gives the Chinese government the power to take over a company's communications equipment. Both companies have apparently engaged in conduct like intellectual property theft, bribery, and corruption. And an independent cybersecurity firm recently found that over half of the Huawei firmware images they analyzed had at least one potential backdoor and that each Huawei device they tested had an average of 102 known vulnerabilities.

There is no sign that they will cease these patterns and practices. With this and other evidence, it's not hard to see the threat that companies like Huawei and ZTE pose to our networks and to our national security. And because 5G networks are interconnected, even a small amount of compromised equipment could be devastating to a country's national security. 5G means that we must secure our networks from the "core" to the "edge."

At the FCC, we are in a position to do something about this threat. And we are. Just last week, my colleagues and I voted to prohibit carriers from using federal dollars to purchase any equipment or services from companies that pose a national security threat, including Huawei and ZTE.

We are not stopping there. In 2018, I called on the FCC to expand our proceeding and put even more options on the table, including the removal of potentially insecure equipment that carriers have already installed in their networks. After all, if equipment poses a threat, it's not enough to stop subsidizing it: it must come out of the network. I am glad that my colleagues joined me in voting in favor of doing just that last week. So the FCC will continue to eradicate the threat posed by insecure equipment in 5G networks.

Importantly, this discussion is not just about network security in some narrow, technical sense. It is also about what I have described as "5G values"—values that China very clearly does not share. Indeed, President Xi Jinping told security officials in January that China does not walk the "Western road" of constitutionalism, separation of powers, or judicial independence. And that's an understatement. Chinese tech companies have a track record longer than a CVS receipt of illegal and malign conduct, which includes violating sanctions, stealing intellectual property, reported lying about extensive partnerships with military and intelligence entities, and enabling extensive and oppressive state surveillance activities.

So part of this conversation—and similar ones taking place across the globe—is about our shared 5G values. We need to work together to ensure that the companies supplying the equipment and services integral to 5G networks are ones we can trust, and are ones that share our commitment to transparency, rule of law, freedom, and individual rights.

I am pleased to report that we are now seeing many countries recognize this position. In March, for instance, the European Commission released a set of recommendations to improve 5G security, which include assessing the risk that equipment vendors could be influenced by third party countries. More recently, in May, the Czech Republic hosted representatives from more than 30 countries to build a common approach to 5G security. That effort produced the Prague Principles, which are a set of recommendations on how to build a secure and trustworthy 5G network. Those principles also recognize the risks posed by a third country wielding influence over an equipment supplier. Australia issued 5G security guidance to protect their networks from unauthorized access or interference by "vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law." Japan has imposed requirements to "take appropriate cyber security measures including measures to respond to supply chain risks." Taiwan has extended its existing measures regarding trusted equipment vendors to cover all 5G government networks and critical infrastructure. And most recently, U.S. Vice President Mike Pence and Polish President Andrzej Duda signed a Memorandum of Understanding on 5G security.

So we have seen a great deal of progress on securing 5G networks over the course of the past year. I am confident that this progress will continue. And I look forward to answering any questions you may have.