STATEMENT OF
COMMISSIONER BRENDAN CARR

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Program*, WC Docket No. 18-89.

Earlier this year, I had the privilege of visiting Malmstrom Air Force Base near Great Falls, Montana. I spent time there with Colonel Jennifer Reeves who is Commander of the 341st Missile Wing. Colonel Reeves and her team have one of the most significant and weighty missions in government. In their charge are150 intercontinental ballistic missiles loaded in underground silos spread across northern Montana. These are missiles that when launched can carry nuclear warheads almost 10,000 miles. Colonel Reeves told me that her job is to make sure they're always ready to go. Set against that destructive power is a completely serene and wide-open landscape—it's just wheat fields and Big Sky Country. Except as it turns out, there are cell towers all around the Montana missile fields running on Huawei equipment.[1] I got a firsthand look at those when I was up there.

This is not just a concern for the military. Everything we do in modern society 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. 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, and that government agencies remain vigilant and focused on the threat. Last year's National Defense Authorization Act prohibited government agencies and contractors from using Chinese equipment. The Department of Commerce has clamped down on the Chinese firms' abilities to do business with U.S. firms. Last year, we launched this proceeding to do our part to ensure U.S. national security. And this month Attorney General William P. Barr wrote to the Commission that, "we should not signal that Huawei and ZTE are anything other than a threat to our collective security."

When combined with the ever increasing sophistication of cyber attacks and the fact that attacks from state actors are by far the most well-funded and advanced, it's not hard to see the threat that companies like Huawei and ZTE pose to our networks and to our national security. Indeed, China's National Intelligence Law requires that all "organizations…cooperate with the State intelligence work," and it provides them no right to refuse.[2] It also gives the Chinese government the power to take over a company's communications equipment.[3] And because the networks in the U.S—from rural America to big city—are interconnected, even a small amount of compromised equipment could be devastating to U.S. security.

At the FCC, we are in a position to do something about this threat. And we are. Today, we are prohibiting carriers from using federal dollars to purchase any equipment or services from companies that pose a national security threat, including Huawei and ZTE.

And 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 covered equipment that carriers have already installed in their networks. That would include some of the equipment I saw out in Montana. 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 we are moving forward with that idea and proposing to take that action today.

---

[1] Alex Marquardt and Michael Conte, *Huawei Connects rural America. Could it threaten the country's most sensitive military sites?* CNN, (Mar. 11, 2019) https://www.cnn.com/2019/03/11/politics/huawei-cell-towers-missile-silos/index.html.

[2] Chinese National Intelligence Law, Article 7.

[3] Chinese National Intelligence Law, Article 17.

I also want to thank my colleagues for agreeing to expand the scope of today's Further Notice. We now go beyond the initial proposal, which focused on removing equipment if the carrier receives federal support, to asking whether we should mandate the removal of covered equipment regardless of whether the communications provider receives federal support. I appreciate that my colleagues not only supported that suggestion but called for similar edits.

Today, the U.S. has the leading 5G networks in the world. And today's decision will help extend American leadership by ensuring the security of these vital networks.

I want to thank the staff of the Wireline Competition Bureau for their work on this item. It has my full support.