STATEMENT OF
COMMISSIONER BRENDAN CARR

Re: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program,* ET Docket No. 21-232; *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, EA Docket No. 21-233.

In 2019, 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 are 150 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.

By now, I scarcely need to explain why the presence of Chinese-state backed communications equipment operating near American missile silos is concerning. Indeed, it is easy to understand that the Chinese government would value direct access to our telecom networks for reasons contrary to our security interests and our democratic values.

Thankfully, the United States has taken decisive actions to protect Americans from threats posed by entities owned or controlled by Communist China. In 2018, Congress placed a ban on the use of federal funding to purchase this untrustworthy equipment through the National Defense Authorization Act. That same year, I worked with my colleagues to expand the scope of the FCC's network security Notice of Proposed Rulemaking to put additional options on the table, including the removal of covered equipment—or as it has come to be known, rip and replace. And just last year, the FCC adopted rules for that rip and replace effort. In doing so, we also established the FCC's Covered List to designate entities that pose an unacceptable risk to our national security. So far, we've determined five companies—Huawei, ZTE, Hytera, Hikvision, and Dahua—meet this threshold.

Although our rip and replace requirement is a significant step towards strengthening our national security, it is limited to gear that is funded through our Universal Service Fund. The FCC's rules expressly allow the continued installation of this equipment, so long as federal dollars are not involved. This is a glaring loophole, and one that Huawei and others are using today. It is the presence of this insecure equipment in our equipment that is the threat, not the source of funding used to purchase it. Yet the FCC, through its equipment authorization process, continues to approve for use in the U.S. thousands of applications from Huawei and other entities deemed national security threats. The FCC has approved more than 3,000 applications from Huawei alone since 2018. And just this month, the FCC approved applications from Hytera Communications.

Once an entity lands on our Covered List, there appears to be no reason why the FCC should continue to review its gear and offer the FCC's seal of approval. Taking this step, as I first proposed in 2019 and then expanded on in March of this year, will strengthen our national security by preventing the further installation and use of insecure technology in our networks.

So I want to thank Acting Chairwoman Rosenworcel for her leadership on this national security issue. I am pleased we are taking meaningful action towards closing this loophole. Indeed, the rules we propose are simple: equipment from entities that pose a national security risk will no longer be eligible for FCC approval. We also seek comment on ways to ensure compliance with these rules and on the enforcement tools that may be appropriate for those who fail to live up to them.

We are launching this proceeding with a simple and important goal in mind—to protect America's communications networks and, in turn, our national security. But at the same time, this is also about what I have described as our "5G values"—values that Communist China clearly does not share with the United States or other democratic nations around the world. I am pleased that my FCC colleagues and I are working together to ensure that the companies supplying equipment integral to our networks are ones we can trust, and are ones that share our commitment to transparency, rule of law, and human rights.

I am also encouraged that bipartisan, bicameral legislation, known as the "Secure Equipment Act," has been introduced by Senator Marco Rubio, Senator Ed Markey, House Republican Whip Steve Scalise, and Congresswoman Anna Eshoo. The Secure Equipment Act recognizes the urgent need for the Commission to secure our networks through this proceeding and I commend these Members of Congress for their bold leadership.

I would like to thank Acting Chairwoman Rosenworcel again for bringing this item forward and to my colleagues for their work on it.

Finally, I want to express my thanks to staff in the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau for their work in preparing this item. It has my support.