## STATEMENT OF COMMISSIONER BRENDAN CARR

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

We launched this proceeding nearly three years ago with a simple and important goal in mind—to protect America's communications networks and in turn our national security. After all, if our communications networks are threatened, everything we value is threated.

Before we voted on the Notice of Proposed Rulemaking back in April 2018, I asked my colleagues to broaden the scope of our proceeding and put additional options on the table. In addition to prohibiting carriers from using USF funds to purchase insecure equipment on a going forward basis, I suggested that we seek comment on removing any insecure gear that may already be in our communications networks.

Flash forward to today and the national security threats posed by allowing this type of covered equipment to remain in our networks has only grown. Indeed, I can think of no greater threat to our security than the one now posed by Communist China and those that would do its bidding.

The record on this is clear: The Chinese government intends to surveil persons within our borders, for government security and spying advantage, as well as for intellectual property and an industrial or business edge. The New York Times has reported that hackers working for the Chinese government stole some of our government's most important cybersecurity tools and repurposed them to attack Western allies and businesses. The Chinese reportedly targeted one of our ally's telecom networks, and when the tools were later transferred to North Korea and Russia, those governments crippled British hospitals and shipping companies. They even shut down a Ukrainian airport, its postal service, gas stations, and ATMs. There is little doubt that the Chinese government would value additional direct access to our telecom networks for reasons contrary to our security interests.

Under Chairman Pai's leadership, the FCC has shown the strength and resolve to meet this threat. We have issued Show Cause Orders to companies that are owned and controlled by the People's Republic of China. We have blocked one such company from connecting to our networks. We have prohibited companies that have been barred from bidding on federal contracts for national security reasons from participating in our spectrum auctions. And we have established CSRIC as an advisory council charged with providing recommendations to ensure the security of our communications networks, among other actions.

America has turned the page on the weak and timid approach to Communist China of the past. Any backsliding or softening of our approach would be a monumental mistake.

So today, with new authority from Congress, we implement the process for removing insecure equipment that is already installed in networks throughout the country. There will be plenty of difficult work ahead to fully implement and fund the replacement efforts, and Congress has already begun to work on the funding challenge with the Ensuring Network Security Act, which, if passed would help us ensure America has the most secure 5G networks in the world.

And it is imperative that we build on our actions today. Just last month, the Executive Branch submitted filings detailing their review of China Unicom and Pacific Networks—two entities that hold Section 214 authorizations and that are ultimately owned by the PRC. The Executive Branch's public filings detail a nefarious pattern of economic espionage and trade secrets theft. They cover charges demonstrating "at a granular level how the PRC uses all available levers to steal sensitive U.S. person data, trade secrets, and other commercially valuable information." And they outline the steps some of these entities have been taking to extend their operations in the U.S.

So our work at the FCC must continue. The FCC should build on the leadership we have shown and take immediate and appropriate action on the China Unicom and Pacific Networks authorizations.

Thank you to the staff of the Wireline Competition Bureau and the Public Safety and Homeland Security Bureau for their hard work on this and the many other important national security items that they have worked on. This decision has my support.