STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, (December 10, 2020)

Our 5G future is about connecting everything. It is about moving to a new networked world that will open up possibilities for communications that we cannot even fully imagine today. By exponentially increasing the connections between people and things around us, this technology could become an input in everything we do—improving agriculture, education, healthcare, energy, transportation, and more. The data we derive from all of these connections is powerful. It will inform machine learning, artificial intelligence, and the next generation of innovation across the economy.

This is exciting. But these opportunities also bring big security challenges. That's because they create a broader attack surface for cyber events, with more devices and a huge increase in traffic load. So we need networks that are trustworthy, resilient, and secure—and we need them right now. And we will not have secure networks in the United States if we do not first have a secure communications supply chain.

That is why what the Federal Communications Commission does today is important. We take another step in our multi-year effort to secure the communications supply chain. Specifically, we put in place a system to replace insecure equipment from the Chinese companies Huawei and ZTE, to the extent that it is present in our networks today. This is critical because we know that there are vulnerabilities that come with this equipment—and those vulnerabilities could provide foreign interests with access to our networks and jeopardize the security of communications in the United States. But while we authorize this effort today, to implement it in full requires an appropriation from Congress, consistent with the Secure and Trusted Communications Networks Act. As this decision demonstrates, we are ready.

But we can't stop here. This is only the beginning. Because we have so much more work to do to ensure that our communications future is secure. China is playing the long game. By using state-sponsored technological development to extend its economic reach, it could put itself in a position to gather intelligence, steal intellectual property, and bring down regional communications in times of crisis. And despite our efforts here, the Chinese government is still actively consolidating its global 5G authority. It has been funding and building infrastructure across Africa, Latin America, and Central and Southeast Asia. It is a central player in writing international standards and securing patents for emerging 5G technologies. It is developing trade alliances like the Regional Comprehensive Economic Partnership that could sustain its advantages in international supply chains and create more opportunities for Huawei and ZTE to produce and sell within the region.

What does this mean? It means what we do here —banning two vendors and removing their equipment from our nation's networks—is a start, but it is not enough. The United States needs a more comprehensive approach to secure 5G—both at home and abroad.

First, we need a coordinated national strategy for 5G security. Just two months ago the Government Accountability Office warned that there are serious deficiencies in our present national security plan developed pursuant to the Secure 5G and Beyond Act. We need to do better. When we do, it should include a robust plan for research and development, incentives for carriers to bring next-generation connections to rural and underserved communities so we do not deepen our digital divide, and across-the-board efforts to boost competition. In other words, rather than trying to match the tactics and scale of industrial policy in China, the United States should play to its strengths to help expand the market for secure communications equipment.

Second, we need to stimulate this new market for communications equipment by supporting the development of open radio access network technology here on our shores. Today, most carriers rely on just a few European or Chinese equipment makers to build out their networks—and that market is shrinking. But we can open this ecosystem to new providers by supporting the development of open RAN, which has the potential to increase diversity and competition in communications equipment. In this new market we can make security a priority and not an afterthought. And we may be able to do so at lower cost, making this virtualized equipment more competitive with state-subsidized equipment from Huawei and ZTE. On top of that, it pushes the equipment market to where the United States is strongest—in semiconductors and software. The FCC should help this effort by establishing open RAN testbeds that bring together operators, vendors, vertical interests, and government agencies.

Third and finally, we need to address the security challenges posed by Chinese equipment by building a consistent and united front with our allies and not alienating them. The United States represents roughly a quarter of global gross domestic product. When we lock arms with other like-minded nations, we are stronger. So let's not go at this alone. Let's build on multilateral efforts like the Prague Principles and use our collective leverage to shape how communications networks develop and ensure that new technologies honor democratic principles and human rights.

We have our work cut out for us. As this proceeding clearly demonstrates, network security and national security go hand-in-hand. Together, they provide a foundation for 5G innovation and economic security. If we do this right, we will multiply the opportunities we have to support American values in the deployment of next generation communications both at home and abroad. And that is how we engage China from a position of strength—and grow American leadership in digital technology.