STATEMENT OF
ACTING CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Third Further Notice of Proposed Rulemaking (February 17, 2021).

There is no task at this agency—or in any part of the federal government—that is more important than keeping the American people safe. But history demonstrates that no single entity can meet this challenge alone. That is why I am committed to working with our federal partners and the private sector to increase the security and resiliency of our nation's communications networks. Moreover, I am guided by the conviction that working with our allies and multilateral institutions can multiply our strength across the globe. I believe it is time for this agency to revitalize its approach to network security because it is an essential part of our national security, our economic recovery, and our leadership in a post-pandemic world.

So let's get started—right here, right now. In appropriations legislation late last year Congress provided $1.9 billion for the Federal Communications Commission to implement the requirements of the Secure and Trusted Communications Networks Act. This law bolstered this agency's multi-year efforts to secure the communications supply chain, by providing us with the authority to help remove and replace insecure network equipment across the country from the Chinese companies Huawei and ZTE and then reimburse carriers for the cost of doing so. This is critical. That's because we know there are vulnerabilities that come with this equipment and those vulnerabilities could provide foreign interests with access to our networks, jeopardizing the security of communications in the United States.

That brings me to today's rulemaking. It's an effort to harmonize the past work of the agency on this topic with the new requirements in the appropriations legislation. That means raising the eligibility cap for those participating. It means modifying rules about how reimbursement funds can be used. And it means updating prioritization policies in the event that reimbursement costs exceed funding available. But above all, it means getting going. The sooner we conclude this proceeding, the swifter we can start helping providers secure their networks.

But this is only the beginning. The damage from recent supply chain attacks, like the SolarWinds software breach, demonstrates the need for a coordinated, multifaceted, and strategic approach to protecting our networks from all threats. With this new appropriation from Congress, we have an opportunity to do just that. But we also have an opportunity right now to refresh our networks and reinvigorate our approach to network security so that the United States leads in the future of innovation. So we need to meet this moment with more than just a plan to address yesterday's security challenges but with ideas for tomorrow's as well. That is why I have already reached out to my peers in other parts of the federal government to help coordinate and advance our implementation of the law. That includes speaking with present leadership at the National Telecommunications and Information Administration, the Cybersecurity and Infrastructure Security Agency, and the Deputy National Security Advisor for Cyber and Emerging Technology in the new Administration.

While we make it a priority to coordinate externally, we need to do the same internally. So my office is exploring changes to the FCC process for reviewing matters related to national security, which right now are siloed within the agency's various bureaus and offices. If we are going to keep pace with the growing threats to our communications, we need a dedicated interagency and cross-bureau team of experts advancing a comprehensive approach to securing our nation's communications. That work is already underway, and I look forward to the improved decision-making that will result.

For their diligent work to protect our network security and national security, I thank Pam Arluk, Brian Cruikshank, Elizabeth Cuttner, Justin Faulb, Billy Layton, Kris Monteith, and Ryan Palmer of the

Wireline Competition Bureau; Patrick Brogan, Alex Espinoza, Tanner Hinkel, Ken Lynch, Giulia McHenry, Chuck Needy, Eric Ralph, and Emily Talaga of the Office of Economics and Analytics; and Malena Barzilai, Michael Carlson, Rick Mallen, Linda Oliver, and Bill Richardson of the Office of General Counsel.