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.

In the United States, our communications systems are built on trust. We trust that our calls go through. We trust that our connections are free of unlawful surveillance. We trust that our networks are open to all without threat to national security or fundamental human rights.

This trust in our communications systems is essential. But sustaining it requires effort. It requires that we identify threats to this trust and take actions to address them—and that is what we do today.

To understand why requires a bit of explanation. Several years ago, the Federal Communications Commission began an effort to prevent insecure equipment, like that from Huawei and ZTE, from being used in communications networks supported by our universal service programs. We recognized then what we know clearly now: there is a serious risk that this equipment may be manipulated, disrupted, or controlled by foreign actors. Its presence threatens the very trust we require in our communications systems.

Congress chose to address this threat more broadly by setting an ambitious goal: removing this equipment from our communications networks, wherever it may exist. It came up with a plan for achieving this goal in the Secure and Trusted Communications Networks Act. Later, it appropriated nearly $1.9 billion to see the plan through. Then, in the Consolidated Appropriations Act of 2021, it adjusted the plan to ensure this goal is fully realized.

As a result of this legislative activity, the FCC will soon undertake what is perhaps the most significant federally funded effort to rebuild and secure commercial communications networks nationwide. This means we will evaluate network after network, base station after base station, and router after router until we have rooted out equipment that could undermine our national security.

It's a daunting task. That's because removing insecure equipment from existing networks after installation is hard. Historically, these systems are closed and deeply integrated, with little opportunity to mix and match equipment from different vendors. But going forward we can do this differently. Most importantly, undertaking this process provides us with an opportunity to demonstrate for the world how to build a more secure future for 5G networks.

Tackling a big goal like this requires many small and consistent steps. In December, with my predecessor at the helm, this agency adopted its first rules implementing the Secure and Trusted Communications Networks Act. In February, we proposed changes in order to incorporate amendments to the law that were adopted in the Consolidated Appropriations Act of 2021. In March, we released a draft catalog itemizing expenses and suggesting replacements for insecure equipment. In April, we selected an administrator to run the nearly $1.9 billion Reimbursement Program. In May, we sought further comment from stakeholders about outstanding program details.

That's a lot of forward steps. Today we take another important one. We put the finishing touches on the Reimbursement Program. Specifically, we harmonize the past work of this agency with new appropriations legislation. This means raising the eligibility cap for those participating. It means modifying rules about how reimbursement funds can be used. It also means updating prioritization policies in the event that reimbursement costs exceed available funding.

But above all, it means we are getting going. In fact, with this step underway, I am pleased to announce that October 29 is now our target date for opening the filing window for the Reimbursement Program. That means carriers can start planning for their applications and their new networks.

There's a lot of work to do. As we strive to meet this target, the FCC will continue our work to ensure that secure alternatives exist. We want companies cutting out high-risk hardware from their networks to have the opportunity to use trusted alternatives, including traditional end-to-end proprietary gear as well as promising newer alternatives, like interoperable open radio access network solutions, or open RAN. In fact, on Wednesday of this week the FCC will hold a two-day virtual open RAN showcase that will give network operators interested in the Reimbursement Program an opportunity to hear directly from vendors whose interoperable, open interface, standards-based 5G network equipment and services will be ready and available for purchase and installation this year. This showcase is an opportunity to jump-start United States innovation in this critical technology.

Thank you to my colleagues for their support for today's effort and their understanding that trust in our communications networks is essential. Thank you also to the staff who worked on this initiative, including Pam Arluk, Allison Baker, Ahuva Battams, Callie Coker, Brian Cruikshank, Elizabeth Cuttner, Justin Faulb, Victoria Goldberg, Christopher Koves, Billy Layton, Lee McFarland, Kris Monteith, Ryan Palmer, Doug Slotten, Gil Strobel, and Moriah Windus of the Wireline Competition Bureau; Garnet Hanley, Kari Hicks, Robert Krinsky, George Leris, Charles Mathias, John Schauble, Blaise Scinto, and Sean Spivey of the Wireless Telecommunications Bureau; Charlene Goldfield, Jeffery Goldthorp, Deb Jordan, Nikki McGinnis, Zenji Nakazawa, and Austin Randazzo of the Public Safety and Homeland Security Bureau; Patrick Brogan, Tanner Hinkel, Eugene Kiselev, Kenneth Lynch, Chuck Needy, Eric Ralph, and Emily Talaga of the Office of Economics and Analytics; Maura McGowan of the Office of Communications Business Opportunities; Dan Daly and Mark Stephens of the Office of Managing Director; and Malena Barzilai, Michele Ellison, Andrea Kelly, Doug Klein, Rick Mallen, Bill Richardson, and Chin Yoo of the Office of General Counsel.