**STATEMENT OF**
**CHAIRWOMAN JESSICA ROSENWORCEL**

Re: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*; *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, ET Docket No. 21-232, EA Docket No. 21-233, Report and Order, Order, and Further Notice of Proposed Rulemaking

Communications networks are a part of everything we do. We use them to connect with family and friends. We use them to build commercial businesses and civil society. We use them for healthcare and education. We use them to make purchases, seek out news, and get the facts we need to make decisions about our lives, our communities, and our country.

It's a lot and it's why the security of our communications networks matters more than ever before. Yet the truth is we are just getting started. Because in the not-too-distant future these networks will expand to connect everything around us. They will open up possibilities for communications and computing that we cannot even fully imagine today. By exponentially increasing the connections between people and things, communications technologies could become an input in everything we do—improving agriculture, education, healthcare, energy, transportation, and more. The data we will derive from all these connections will be powerful and will inform the next generation of innovation across the economy.

It is essential that we plan for this future right now. That's because we need to ensure the networks we know today become more secure over time and evolve to withstand cyberattack from those who wish to do us harm. After all, with insecure networks it is too easy for bad actors to introduce viruses and malware, steal private data, engage in intellectual property theft, and surveil companies and government agencies.

That is why at the Federal Communications Commission we have made network security a top priority—and we have a long list of accomplishments to show for it.

For starters, we have taken action to improve awareness about network vulnerabilities, threats, and breaches within the federal government and the private sector. On March 12, 2021, we published the first-ever list of communications and services that pose an unacceptable risk to national security as required under the Secure and Trusted Communications Networks Act. This initial Covered List included equipment from the Chinese companies Huawei, ZTE, Hytera, Hikvision, and Dahua. Since then, we've added equipment and services from five additional entities. Last year I also proposed stricter data breach reporting rules and worked with the Department of State to improve how we coordinate national security issues related to submarine cable licenses.

Next, we took concrete action to defend against the threats and vulnerabilities that were identified through our work. We launched the Secure and Trusted Communications Networks Reimbursement Program to remove untrusted equipment from our networks and replace them with secure alternatives. Working with our national security colleagues, we revoked the section 214 operating authorities of four Chinese state-owned carriers who were providing service in the United States. Last month, we required Emergency Alert System and Wireless Emergency Alert System participants to have a cybersecurity risk management plan in place. We also announced a first-of-its-kind settlement against a company that will require it to divest unvetted Russian ownership, pay a civil penalty, and put in place new security procedures to review any new ownership through the Office of Foreign Asset Control at the Treasury Department.

Finally, we took steps to build security into what comes next. We launched new inquiries on the security of internet routing and the Internet of Things. I recharted the Communications Security, Reliability, and Interoperability Council and, for the first time, designated the Cybersecurity and Infrastructure Security Agency as co-chair. And I revitalized the Cybersecurity Forum for Independent and Executive Branch Regulators to share information and expertise and enhance the cybersecurity of the nation's critical infrastructure.

Together, these efforts will make our networks more secure. But today we go a step further, by addressing not just communications but the process we use to authorize communications equipment in the United States.

Let me explain. While we've flagged equipment as posing a national security risk, prohibited companies from using federal funds to purchase them, and even stood up programs to replace them, for the last several years the FCC has continued to put its stamp of approval on this equipment through its equipment authorization process. So long as this equipment carries that stamp, it can continue to be imported into the United States and sold to buyers who are not using federal funds.

But that does not make any sense. After all, there is little benefit in having these lists and these bans in place just to leave open other opportunities for this equipment to be present in our networks. So today we are taking action to align our equipment authorization procedures with the rest of our national security policies.

Specifically, under the rules we adopt today pursuant to the Secure Equipment Act, the FCC will no longer authorize equipment that is on the Covered List because it poses an unacceptable risk to the national security of the United States or the safety of United States persons. That includes telecommunications and video surveillance equipment from Huawei and ZTE. It also includes telecommunications and video surveillance equipment from Hytera, Hikvision, and Dahua that is used for the purpose of public safety, security of government facilities, physical surveillance of critical infrastructure, and other national security purposes. For these three companies, we will require them to document what safeguards they will put in place on marketing or sale for these purposes and we are putting in place a freeze on all of their telecommunications and video surveillance equipment authorization applications until that work is done.

The action we take today covers base station equipment that goes into our networks. It covers phones, cameras, and Wi-Fi routers that go into our homes. And it covers re-branded or "white label" equipment that is developed for the marketplace. In other words, this approach is comprehensive.

However, because we recognize that these issues may evolve over time, we also adopt a further rulemaking to invite additional comment on the need to update our equipment approval process to address component parts. We also ask how and if it is necessary to consider the revocation of any existing authorization for covered equipment in the future.

This order and rulemaking is part of our broader focus on network security and I am grateful for the support of my colleagues Commissioner Carr, Commissioner Starks, and Commissioner Simington in this effort. I also want thank the Congressional champions of the Secure Equipment Act, including Senator Markey, Senator Rubio, Congresswoman Eshoo, and Congressman Steve Scalise, for their support for the work of this agency and laser-like focus on the steps we can take to address insecure communications and network equipment.