STATEMENT OF CHAIRWOMAN JESSICA ROSENWORCEL

Re: *China Unicom (Americas) Operations Limited*, GN Docket No. 20-110, ITC-214-20020728-00361; ITC-214-20020724-00427

Today we take another critical step to protect our communications networks from foreign national security threats. We direct China Unicom Americas to discontinue any domestic or international services that it provides pursuant to its section 214 authority.

We reach this decision carefully. To understand why requires a bit of history.

It was more than two decades ago that China Unicom Americas first received section 214 authorization from the Federal Communications Commission to provide domestic and international service in the United States. But since that time, the national security landscape has shifted and there has been mounting evidence—and with it, a growing concern—that Chinese state-owned carriers pose a real threat to the security of our telecommunications networks.

As a result, in 2019, the Commission denied China Mobile USA the authority to enter the United States market for national security reasons. In 2020, the Senate Permanent Subcommittee on Investigations issued a report on the threats associated with Chinese state-owned carriers operating in the United States.

At roughly the same time, the FCC took steps to consider the threat posed by China Unicom Americas. That's because China Unicom Americas shares the characteristics highlighted by our national security agencies with respect to China Mobile USA. Accordingly, the International Bureau, the Enforcement Bureau, and the Wireline Competition Bureau issued an Order to Show Cause to China Unicom Americas that directed the company to demonstrate why the agency should not initiate a proceeding to revoke its domestic and international section 214 authority.

Once China Unicom Americas responded, the FCC reached out to its national security partners for their perspective and expertise. We asked the Department of Justice, on behalf of the Attorney General, to address the arguments made by China Unicom Americas in its response to the Order to Show Cause. The Executive Branch, represented by NTIA, responded to the letter and provided their view that China Unicom Americas was subject to the control of the Chinese Government.

At each stage in the process, China Unicom Americas had an opportunity to respond. And at each stage, China Unicom Americas' responses were incomplete, misleading, or incorrect.

As a result, last year we found that China Unicom Americas failed to dispel those concerns regarding the retention of its authority to provide telecommunications services in the United States. And we provided China Unicom Americas another opportunity to make its case. We also sought additional guidance from our partners in the Executive Branch before reaching our decision today.

On the basis of this record, we believe it is clear that the public interest is no longer served by China Unicom Americas' retention of its section 214 authority. So we revoke China Unicom Americas' domestic and international section 214 authority and direct China Unicom Americas to discontinue within 60 days of the release of this order any domestic or international services that it provides pursuant to this authority.

Of course, this isn't the first time we've taken action to withdraw section 214 authority to protect our communications infrastructure from the threat posed by Chinese state-owned carriers. In 2021, we revoked China Telecom Americas' prior authorization to provide service within the United States. We also have started similar revocation proceedings against two other companies, Pacific Networks Corp. and ComNet (USA) LLC.

Today's action is the latest in a series of steps we've taken to keep our networks secure. In the last year, we have pursued a multi-faced approach to protect communications and strengthen our national security.

We are making our supply chains more transparent. In March of last year, the FCC published the first-ever list of communications equipment and services that pose an unacceptable risk to national security. This is known as the Covered List. Congress gave our national security and law enforcement agencies the primary responsibility to determine what equipment and services should be added to this list over time. So this month I sent letters to the Department of Commerce, the Office of the Director of National Intelligence, the Federal Acquisition Security Council, the Department of Justice, and the Federal Bureau of Investigation so that we can update the Covered List by March of this year. That means we will very shortly confirm the status of other companies that have been the subject of recent security attention. But it's not enough to know what the risk is, we need to know where it is, too. So we are also getting ready to launch a new data collection under the Secure and Trusted Communications Networks Act that will require providers to report whether or not they have equipment or services on the Covered List.

We are locking down our universal service programs. We've prohibited the use of funds from these programs to purchase equipment on our Covered List.

We are replacing insecure equipment in our networks. In October, we launched a \$1.9 billion program to remove equipment from Huawei and ZTE to the extent that it is present in our domestic networks today. In doing so, we created opportunities to transition to Open RAN systems, which will help diversify the technology in our networks and support a market for more secure 5G equipment.

We are reviewing submarine cables with greater care. We have worked with the Department of State to change the 20-year-old process used for approving licenses for submarine cables. The revised approach better incorporates the new Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector into the assessment process. There will be no rubber-stamping applications. Instead, we have careful review.

We are updating our equipment authorization process. We have proposed rules that will align our equipment authorization procedures with our national security policies and ensure that going forward the FCC will not approve equipment from any companies on the Covered List.

We are reducing cyber risk. In light of recent data breaches, we have proposed stricter data breach reporting rules. We have launched a Notice of Inquiry on security of the Internet of Things. And we are rechartering the Cybersecurity Regulators Forum that has been dormant for the past few years—and assuming its leadership.

We are keeping 5G security front of mind and working with new partners to do so. We rechartered the Communications, Security, Reliability, and Interoperability Council and gave it a 5G focus. And for the first time, CSRIC is being co-chaired by the Cybersecurity and Infrastructure Security Agency—so we have a whole-of-government approach to 5G security.

These initiatives cut across the work of the agency. That's not an accident. Last year, I established the National Security Policy Committee, a dedicated, cross-bureau team of experts advancing a comprehensive approach to security matters at the FCC. The work they've done in the last year is thoughtful and impressive—and there's more to come.

Thank you to the staff who worked on today's decision, including Denise Coca, Kate Collins, Francis Gutierrez, Jocelyn Jezierny, Gabrielle Kim, David Krech, Wayne Leighton, Tom Sullivan, and Troy Tanner from the International Bureau; Eduard Bartholme, Michael Snyder, Mark Stone, and Patrick Webre from the Consumer and Governmental Affairs Bureau; Jeffrey Gee, Rosemary Harold, Pam Kane, and Christopher Killion from the Enforcement Bureau; Bob Cannon, Catherine Matraves, Deena Shetler, Emily Talaga, and Virginia Metallo from the Office of Economics and Analytics; Padma Krishnaswamy from the Office of Engineering and Technology; Ken Carlberg, Lisa Fowlkes, Jeffery Goldthorp, Deb Jordan, and Nicole McGinnis from the Public Safety and Homeland Security Bureau; Pam Arluk, Michele Berlove, Melissa Droller Kirkel, Jodie May, Rodney McDonald, Kris Monteith, and Terri Natoli from the Wireline Competition Bureau; Garnet Hanly and Susannah Larson from the Wireless Telecommunications Bureau; and Matthew Dunne, Michele Ellison, Doug Klein, Jacob Lewis, Scott Noveck, Bill Richardson, Joel Rabinovitz, and Royce Sherlock from the Office of General Counsel.