STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *China Unicom (Americas) Operations Limited*, GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427;
Pacific Networks Corp. and ComNet (USA) LLC, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199.

As we move toward a more interconnected future, the Commission must protect the integrity of our networks. Today, we take another important step in ensuring American networks are guarded against adversary state-owned or controlled carriers by initiating a proceeding to revoke the authority of China Unicom Americas, Pacific Networks and its wholly owned subsidiary, ComNet, to operate in the United States.

Today's decisions further our commitment to preserving the safety and security of our communications. Over the last two years, the Commission has rejected an application from the U.S. subsidiary of China Mobile, the largest mobile provider in the world, and initiated a proceeding to revoke U.S. operating authority from China Telecom Americas, the U.S. subsidiary of China's largest telecom provider. Like those carriers, the companies that are the subject of today's actions are ultimately owned and/or controlled by the Chinese government and therefore vulnerable to its exploitation and control, creating a significant threat to our national security and law enforcement interests.

These companies are required under Chinese law to disclose sensitive customer information upon demand to assist government intelligence activities. They've also demonstrated a lack of transparency and reliability in previous dealings with the Commission and Team Telecom. For example, both companies failed to comply with Commission rules concerning disclosure of ownership changes and company reorganization, and they failed to provide crucial information concerning their affiliations with the Chinese government and cybersecurity practices. According to Team Telecom, there are no mitigation measures that could enable the companies' continued operation in the United States.

Our actions represent a bipartisan consensus across the federal government that American communications must be protected from companies owned or controlled by the Chinese government. Our responsibilities don't stop at the border. As I stated last year, international undersea cables carry 99% of the world's data traffic, and Chinese companies and their American partners are actively seeking to increase the number of cables connecting our countries. As we saw with the withdrawal of an undersea cable application just one week ago connecting California and Hong Kong, however, applicants are coming to understand that the Commission and its federal partners will not approve any application that fails to guarantee the fundamental security of American communications from any tampering, blocking, or interception by adversary states or other bad actors.

All of these issues highlight another security threat to our communications and privacy. Even as we act to remove or block Chinese telecom carriers from accessing U.S. networks, many of these same companies also own data centers operating within the United States, including multiple locations in metro areas like the Washington, DC area, New York City, and Los Angeles.[1] As the Department of Homeland Security has warned, these data centers leave their customers vulnerable to data theft for one of the same reasons we act today – Chinese law requires these companies to secretly share data with the Chinese

[1] *See, e.g.,* China Telecom Data Center Locations, https://www.datacenters.com/china-telecom-data-center-locations (last visited Mar. 12, 2021).

government or other entities upon request, even if that request is illegal under U.S. law.[2] Currently, the FCC lacks the authority to address this potential national security threat, but as part of any review of our jurisdiction over broadband services generally, the Commission should work with the new Administration and Congress to consider whether the FCC needs broader jurisdiction to tackle this emerging network security issue as well.

Thank you to the staff of the International Bureau for their work on these items.

[2] *See* U.S. Dept. of Homeland Security, Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China (rel. Dec. 22, 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.