

**STATEMENT OF
COMMISSIONER GEOFFREY STARKS**

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

From the basic convenience of wireless calling to the promise of the metaverse, advanced communications and information service technologies are transforming every aspect of our lives. 5G and other advanced broadband technologies are shifting into a new gear, and the race for 6G is already well underway.

But one byproduct of universal, always-on connectivity is the potential vulnerability it creates. As our networks connect with others around the world, we will inevitably encounter bad actors. We must remain on guard against any efforts to intercept, tamper with, or block our communications.

Today's decision is the latest in a series of FCC actions against such threats, and I fully support it. As our order states, the evidence clearly establishes that China Unicom Americas is subject to the exploitation, influence, and control of the Chinese government. As such, the company is highly likely to be forced to comply with Chinese government requests – including the disclosure of communications by American citizens – without sufficient legal protections and independent judicial oversight. Moreover, the company's actions during this investigation, including its failure to provide accurate and truthful information to the Commission, further demonstrate that China Unicom Americas simply cannot be trusted to provide telecommunications service in the United States. Our decision to revoke the company's authority to provide such service makes us more secure.

But there is more work to do. For example, data centers have become critical parts of the American communications and technologies sectors and are instrumental to new use cases like edge computing. As I've noted previously, however, even after loss of their section 214 authority, companies like China Unicom Americas can continue to offer data center services to American customers. The Department of Homeland Security has warned that these data centers leave their customers vulnerable to data theft for one of the same reasons underlying our decision today – these companies are legally required to secretly share data with the Chinese government or other entities upon request, even if that request is illegal under U.S. law. While the FCC currently lacks jurisdiction to address this potential national security threat, we should work with the Administration and Congress to examine whether the Commission needs broader authority to tackle this and other network security threats.

Thank you to the staff of the International Bureau for their work on this item.