STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Pacific Networks Corp. and ComNet (USA) LLC,* GN Docket No. 20-111; ITC-214-20090105-00006; ITC-214-20090424-00199.

Our network security has never been more important. As events in Ukraine continue to unfold, reports indicate that hackers acting on behalf of Russia are seeking to sabotage Ukraine's networks – utilizing new ways of attacking critical infrastructure, financial, and governmental networks, both in cooperation with other hackers and on their own.

While we have yet to see a coordinated attack on American networks, we cannot ignore the capabilities of Russian state actors, which one technology company estimates are responsible for nearly 60 percent of all state-sponsored cyberattacks.[1] The Cybersecurity and Infrastructure Security Agency (CISA) and the FBI recently issued a joint Cybersecurity Advisory urging organizations to take precautions against the destructive malware that has been used to target Ukrainian organizations, and CISA has updated its "Shields Up" webpage to include new cyber services and resources, recommendations, and information on how to protect critical assets. Just last week, I met with CISA's Executive Assistant Director for Cybersecurity to discuss these efforts and how our agencies can continue to work together to address threats to our nation's telecom networks.

I'm proud to say that the FCC is stepping up. I support the Chairwoman's efforts to expand our inter-agency cyber coordination and strengthen our data breach rules. I also strongly support our recent Notice of Inquiry seeking comment on security vulnerabilities of the Border Gateway Protocol (BGP), which bad actors can exploit to misroute traffic for monitoring or interception.

While Pacific Networks and ComNet don't appear to have BGP misrouting capabilities, they pose a threat similar to their fellow Chinese carriers. Like China Unicom Americas, China Telecom Americas, and China Mobile USA, Pacific Networks and ComNet are ultimately owned by a Chinese state entity, and are subject to the exploitation, influence, and control of the Chinese government. As such, they are highly likely to be forced to comply with Chinese government requests – including the accessing, monitoring, and disrupting of U.S. communications. Moreover, Pacific Networks and ComNet have failed to provide complete and accurate information to Congress and the Commission. In total, the companies' actions clearly demonstrate that they cannot be trusted to provide telecommunications service in the United States, and I support our action today.

It was almost 3 years ago that we first acted against a Chinese carrier seeking to operate in the United States. Today's decision revokes the section 214 authority for the last Chinese carriers in our country identified by Team Telecom. Taken as a whole, our actions have strengthened our national security and affirmed the FCC's statutory responsibility to protect the national defense and the safety of life and property.

Network security is national security. Today's action is another positive step towards protecting our national security, but clearly we must continue to rise to the challenges of the day. My thanks to the International Bureau and the other Bureaus and Offices that worked on this proceeding for their hard work on this item.

---

[1] Tom Burt, *Russian cyberattacks pose greater risk to governments and other insights from our annual report*, Microsoft On the Issues (Oct. 7, 2021), https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/.