Opening Statement of Chairman Brett Guthrie
Subcommittee on Communications and Technology
"Global Networks at Risk: Securing the Future of Communications Infrastructure"
Wednesday, April 30, 2025 at 10:00 AM

Thank you, Chairman Hudson for holding this important hearing on the resilience of our communications infrastructure.

Americans are connected to the internet in nearly every aspect of their daily lives. Whether it is for work, staying in touch with loved ones, or receiving healthcare, reliable connectivity is essential. The underlying communications infrastructure is what allows individual Americans and businesses of all sizes to utilize the many digital services that have redefined our economy and society, even if we take them for granted.

Having worked in my family's manufacturing business, I can tell you that it is impossible to operate a business of any size today without access to the internet.

While reliable internet access is important, it must also be secure. That's why this hearing today is so important.

Sophisticated cyber actors, specifically the governments of China, Russia, North Korea, and Iran, directly engage in activities aimed at infiltrating our critical infrastructure, especially our communications networks. These state adversaries and other malicious cyber actors continuously seek to exploit weaknesses in our networks not only to steal sensitive data and commit fraud against Americans, but they also stand to gain sensitive business and government information as they seek to establish footholds for surveillance and future exploitation.

We have seen these efforts play out in recent attacks. We only have to point back to October when Chinese hackers breached the American court wiretap systems. Thankfully, we have so far avoided the worst of the potentially devastating outcomes. But depending on how far they were able to penetrate our networks, our adversaries could also have the capability to cut off our communications services altogether. In other words, they could shut down our mobile and fiber networks, preventing our cell phones and other devices from working. Think about how disruptive—and devastating—that would be to our society.

Our networks are also vulnerable to physical disruptions. For instance, fiber cuts can take months to repair depending on where they're located and even the time of year. If we're talking about subsea cables that are isolated in the ocean, for example, these cuts could interrupt international data flows and result in

degraded service for millions of people over an extended period of time given the relative difficulty of repair.

Increasingly, satellite-provided services are being used to help close the digital divide, and provide positioning, navigation, and timing data for government and private sector users. Foreign adversaries like China and Russia are reportedly developing anti-satellite capabilities, which would cause serious disruption to critical services. In the case of GPS, a satellite-provided service, we have very few alternatives. Disruption to these critical communications services has the potential to cause chaos here in the homeland and reverberate throughout the economy. It could also give our adversaries the ability to disrupt American military mobilization in the event of a conflict or attack.

Securing our communications systems from bad actors has been a longstanding bipartisan priority of this Committee and is essential to preserving our national and economic security. This Committee led the effort to rip and replace untrusted vendor equipment from our mobile networks by passing the *Secure and Trusted Communications Network Act*. We built on those efforts by passing the *USA Telecommunications Act* in 2020 to foster a more competitive market of trusted equipment vendors by promoting Open RAN technology. By diversifying our supply chains and removing untrusted equipment, we can help make our mobile networks more resilient to supply chain shortages and bolster them against bad actors like the CCP and the companies affiliated with them.

More work remains to protect our critical infrastructure and harden these essential services against adversarial threats. We

must remain vigilant in protecting our national security, and that starts with understanding the threats and considering policy changes to counter them.

Thank you to the witnesses for your participation. I look forward to hearing from you about how to protect our communications infrastructure and ensure that the U.S. is prepared to defend against the CCP and other adversaries.

Mr. Chairman, I yield back.