Opening Statement for Chair Cathy McMorris Rodgers
Subcommittee on Communications and Technology
“Securing U.S. Communications Infrastructure”
January 11, 2024

(As Prepared for Delivery)

INTRO

Good morning, and thank you, Chairman Latta.

Cybercriminals are estimated to have made nearly eight trillion in 2023—a number that’s expected to rise to around $10.5 trillion by next year. For Americans, who’ve become accustomed to using the Internet as an essential part of life....

... that means their most personal information is constantly at risk of being exploited by bad actors.

Every day, people are sharing more and more of their information online.

We share our financial information when we pay our bills...

...health information when we schedule a doctor’s appointment, and location information when we search for food or other essential items nearby.

We use the internet to stay in touch with friends and family, continue our education, and open new businesses.

The amount of information we share will continue to increase as our technology becomes more advanced.

It’s vital that we ensure the technology we use every day is safe and secure.

Which is why Energy and Commerce is continuing efforts to advance data privacy protections for Americans.

We need to make sure people are protected from the dangers of unsecure applications collecting their personal information unrestricted, especially apps like TikTok, which is beholden to the CCP.

At the same time, we also need to ensure the security of our overall broadband networks, which are foundational for our economy.

They enhance how people connect and create new opportunities for the hardworking people of this country.

CYBERATTACKS

As we become increasingly connected and more reliant on technology, this digital infrastructure that underpins our connection becomes a target for bad actors.

From phishing scams designed to steal our personal information, to ransomware attacks that extort money from people and businesses…

…and AI-generated threats, which are making it easier and easier for criminals to target Americans.

The list of tools continues to grow and the communications sector, in particular, has long been a target.

2021 saw a fifty-one percent increase worldwide in the number of attacks on communications infrastructure.

In the U.S. alone, there are more than 2,200 cyberattacks on communications infrastructure every day—averaging nearly one attack every 39 seconds.

The range of tools used by cybercriminals is extensive and growing.

FOREIGN INFLUENCE

Both in the United States and across the globe, broadband networks are integral to the functioning of governments, military operations, and essential services.

Foreign actors, particularly those from countries with a track record of state-sponsored cyber activities, are increasingly exploiting vulnerabilities in our infrastructure…

…in order to carry out espionage, cyberattacks, and other activities that compromise our national security.

This is why our efforts to remove equipment sourced from companies, like Huawei and ZTE, which are China-owned and controlled by the CCP, are so important.

In 2020, Congress passed the Secure and Trusted Communications Networks Act to mitigate these vulnerabilities.

The bill established a fund for broadband providers to replace communications network equipment that poses a national security threat.

It is vital that Congress provides the three billion dollars needed to fully fund this effort, and I will continue to work with my colleagues to find a path forward.

We cannot continue to allow China to access our networks or compromise our communications supply chains, especially with the increasing frequency and sophistication of these attacks.

CONCLUSION

Addressing ongoing cyber threats will take an all of the above—rather than a one-size-fits-all—approach…

…one that leverages the expertise of our federal agencies in their specific, unique sectors.

At the same time, we must ensure industry is able to innovate and adapt to evolving threats...

…and that government does not unnecessarily restrict industry with overly burdensome regulations that prevent it from responding swiftly to cyber threats.

This is the best way to build on American technological and communications leadership, strengthen our national security, and win the future.

I look forward to today's hearing and discussing how we will enhance our cybersecurity to protect the digital infrastructure that is vital for every aspect of our lives.

Thank you to our witnesses for being here.

Mr. Chairman, I yield back.