Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Health Chairwoman Anna G. Eshoo

Hearing on "A Safe Wireless Future: Securing our Networks and Supply Chains"

June 30, 2021

Thank you for holding this important hearing, Chairman Doyle and Ranking Member Latta.

Securing our wireless networks is a matter of national security because compromised equipment can lead to surveillance of our communications by our adversaries, including foreign governments. This is why I've made the issue a top priority for over a decade. I first wrote to the FCC on November 2, 2010, about the national security risks created by Huawei and ZTE, and I've remained focused on this issue since then.

I'm pleased to see the many important bills that we'll discuss today, including three bipartisan bills I've led:

- H.R. 2685, the *Understanding Cybersecurity of Mobile Networks Act*, is legislation I authored with Rep. Kinzinger that requires the NTIA to conduct an in-depth study of the cybersecurity of the 2G, 3G, and 4G networks in our country. While there have been many disparate efforts to examine vulnerabilities, we lack a comprehensive understanding of the issue. While 5G and 6G are critical for our telecommunications future, most of our calls, texts, and data still traverse through legacy networks which present threats to the whole network.

- H.R. 3919, the *Secure Equipment Act*, is legislation I partnered with Rep. Scalise to introduce. The bill prohibits the FCC from issuing new equipment licenses to companies on the FCC's list of entities that pose a national security threat. Senators Rubio and Markey have companion legislation in the Senate, and Acting Chairwoman Rosenworcel and Commissioner Carr – a Democrat and Republican respectively – support the bill.

- H.R. 4055, the *American Cybersecurity Literacy Act*, is a bill I introduced with Rep. Kinzinger to require NTIA to develop and conduct a cybersecurity literacy campaign to educate Americans about cyber vulnerabilities and best practices to reduce associated risks. Government is only responsible for approximately 20 percent of cybersecurity and individuals and companies are responsible for 80 percent. Americans can vastly reduce harm experienced by cyberattacks by heeding best practices, and the federal government can help spread knowledge about what people can do to reduce their risk.

I'm also pleased that we'll be discussing the advancement of Open RAN and directing agencies to begin to think about 6G.

I look forward to a productive hearing and I yield back.