Committee on Energy and Commerce
Opening Statement as Prepared for Delivery
of
Full Committee Ranking Member Frank Pallone, Jr.

Hearing on "Safeguarding Americans' Communications: Strengthening Cybersecurity in a Digital Era"

January 11, 2024

Today, this Subcommittee continues its vigilance in overseeing our communications networks and ensuring we are doing all we can to protect them from threats. These threats may come from rogue internet criminals using ransomware to extort money from hospitals, schools, and libraries. Or they may come from foreign adversaries that see our networks and devices as entry points to disrupt our daily life or conduct espionage campaigns.

Protecting our communications networks from these threats is essential because the communications sector underpins a significant part of the American economy. From health care, to energy, to public safety, nearly every facet of American life relies on our nation's communications networks. While the innovations and advancements that these networks enable are remarkable, it also makes these networks – and the devices that run on them – targets.

This will only increase as more devices in our homes are connected. Things like cars, televisions, refrigerators, gym equipment and even lightbulbs and home security systems—if they are connected to the internet, they are vulnerable to cyberattacks. This reality means that even our homes are now subject to a cyberattack. It was recently reported that homes equipped with connected devices can face more than 10,000 attacks a week. These attacks can give criminals insight into our movements and data about our families. They can even allow criminals to take over the device remotely.

So, it's imperative that we understand the cybersecurity risks our networks and devices face to better protect our country and consumers from cyberattacks.

This Committee has focused on cybersecurity on a bipartisan basis. In 2020, we came together to enact my bipartisan Secure and Trusted Communications Networks Act. This law gave the Federal Communications Commission (FCC) the authority to exclude untrusted equipment from our communications networks, after our national security agencies concluded they were a real risk. This was a major step in ensuring our networks are secure from malicious foreign interference, but now this Rip and Replace program needs an additional $3 billion to fully rid our networks of Huawei and ZTE equipment. We must come together again to ensure this program is fully funded.

The Biden Administration and the FCC have also taken action to address cybersecurity in the communications sector. Last March, President Biden released the National Cybersecurity Strategy. It takes several important steps, including shifting the burden of protecting cyberspace away from consumers, small businesses, and local governments to software providers who are better positioned to reduce security risks.

President Biden then released the implementation plan for this strategy last July. It outlines more than 65 cybersecurity initiatives that federal agencies are conducting and timelines for their completion. The plan will be updated annually.

At the FCC, Chairwoman Rosenworcel has taken several critical actions to strengthen cybersecurity and enhance supply chain protections. She recently recharted the Communications Security, Reliability, and Interoperability Council (CSRIC) and relaunched the Cybersecurity Forum for Independent and Executive Branch Regulators, which encourages federal agencies to exchange information to protect critical infrastructure.

The FCC has also proposed a voluntary cybersecurity labeling program for Internet of Things devices so that consumers can easily identify trustworthy devices and make safer purchasing decisions.

Finally, while securing our communications networks – and the devices that rely on them – is imperative, I continue to strongly believe that we must also enact robust federal data privacy protections to complement our cybersecurity efforts. For instance, minimizing the amount of consumer data that our networks and devices have access to could help reduce the consumer impact of cyberattacks.

Last Congress, Chair Rodgers and I worked together to advance data privacy legislation with strong provisions focused on data minimization. With cyberattacks becoming a more common occurrence, minimizing the amount of data collected on consumers is vital, and I remain committed to work on enacting strong privacy protections. It is the only way we can limit the aggressive and abusive data collection practices of Big Tech and data brokers, ensure our children's sensitive information is protected online, and put consumers back in control of their data.

I look forward to hearing from our witnesses about the challenges and potential solutions for securing our communications networks and devices as well as consumer data, and I yield back the balance of my time.