U.S. SENATE COMMITTEE ON
COMMERCE, SCIENCE, & TRANSPORTATION

U.S. Senator Ben Ray Luján

Subcommittee on Communications, Media and Broadband

Hearing on Communications Networks Safety and Security

December 11, 2024

Opening Remarks

This hearing of the Subcommittee on Communications, Media, and Broadband will now come to order. Today, the Subcommittee is convening a hearing on "Communications Networks Safety and Security." Thank you to Ranking Member Thune—and Senator Moran for filling in for him today— as well as Chair Cantwell and Ranking Member Cruz, for working with me to schedule this hearing on such an important topic.

I think every Member on this Committee can agree that there is nothing more important than keeping our communities safe. That's why I have worked with my Commerce Committee colleagues to make our aviation system safer, to prevent roadway fatalities, and to protect consumers from fraud and scams. It is also our responsibility to keep our communications networks safe, to ensure that foreign threat actors like China cannot infiltrate our infrastructure or steal Americans' data.

Currently, our communities—our schools, hospitals, and libraries; our police departments and emergency responders; do not have the resources to defend themselves against foreign adversaries. The Salt Typhoon hack that was discovered last month demonstrates that even the largest corporations in the United States are vulnerable. This attack likely represents the largest telecommunications hack in our nation's history.

There is a lot we still don't know about the damage that was done by the Salt Typhoon hacks. But what we do know is that more must be done to prevent attacks like this in the future. There are outstanding recommendations from federal agencies that must be fully implemented across our networks. This includes standards and best practices recommended by the FCC, Team Telecom, and other federal partners that have been lessons learned from prior attacks and data breaches.

One obvious thing we can do today is get equipment manufactured by companies that collaborate with foreign adversaries out of our networks. Congress passed the Secure and Trusted Communications Networks Act in 2020, making it clear that we understand the vital importance of removing Huawei and ZTE equipment from our every network across the country.

Unfortunately, the “Rip and Replace” program has remained partially unfunded for years, opening up our networks to unnecessary risks and preventable threats. I am hopeful that there is strong bipartisan agreement to fully fund this program through this year’s National Defense Authorization Act, and address one of the major known vulnerabilities facing our networks every day once and for all. We also need to protect our networks at every access point—from phones to cars to even baby monitors.

Critically, this includes the undersea cables that carry traffic across the entire world. As the pressure on our networks continues to increase, it is vital that federal partners do everything in their power to keep bad actors out at every point of the supply chain. We are fortunate to have an expert panel with us today who will speak to the vulnerabilities in our communications system, and how we can address them to protect our constituents.

Mr. James Lewis, Senior Vice President and Director of the Technology and Public Policy Program at the Center for Strategic and International Studies, will speak to how foreign threat actors like China work to infiltrate global telecommunications infrastructure to further their intelligence goals; Mr. Tim Donovan, President and CEO of the Competitive Carriers Association, will discuss how small carriers across the country navigate cybersecurity challenges, including the need to remove Chinese equipment from their networks;

Mr. Justin Sherman, Founder and CEO of Global Cyber Strategies and Nonresident Senior Fellow for the Cyber Statecraft Initiative at the Atlantic Council, will speak to how companies and the federal government keep our networks safe, especially undersea cables; and finally Dr. James Mulvenon, PhD, Chief Intelligence Officer at Pamir Consulting, who Senator Moran will introduce. I look forward to a productive conversation today, and thank you all for being here. With that, I turn to our acting Ranking Member, Senator Moran for his opening statement.