Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Communications and Technology Ranking Member Doris Matsui

Subcommittee on Communications and Technology Hearing on "Global Networks at Risk: Securing the Future of Telecommunications Infrastructure"

April 30, 2025

Thank you, Chairman Hudson.

Today's hearing comes on the heels of Salt Typhoon, one of the worst hacks in U.S. history.

Salt Typhoon is a wake-up call that drives home the vulnerabilities in our communications networks.

These networks are the backbone of modern life– connecting us to businesses, public safety, healthcare, education, and communities.

That's what makes them such a ripe target for attack by malicious actors. And why we must strengthen how we protect this critical infrastructure.

Yet, I fear that we are moving backwards, as the Trump administration won't even own up to its pattern of security failures.

President Trump is defending the indefensible—rallying behind the blunders of his Secretary of Defense, who leaked classified war plans to his wife and brother over an unsecured Signal chat.

Likewise, Trump is standing blindly by his National Security Advisor, and countless other senior officials, who used Signal and personal Gmail accounts to conduct sensitive government business.

The Trump administration is handing highly sensitive data to deeply unserious people, who can't be bothered to follow the law—or basic common sense—when it comes to protecting cybersecurity and keeping sensitive information safe.

The world is watching. Bad actors are ready to take advantage of this administration's gross incompetence.

In Congress, Republicans talk tough about protecting America against foreign adversaries. But talk is cheap. Their refusal to hold the Trump administration accountable—despite serious security breaches—speaks volumes.

Republicans are also staying silent as President Trump slashes our federal cyber workforce, gutting our nation's capability to prepare for and respond to attacks on our critical infrastructure.

As one of his earliest acts in office, President Trump disbanded the Cyber Safety Review Board, leaving in limbo our investigation into the largest telecommunications hack in U.S. history.

Instead, Salt Typhoon remains active, as this administration jeopardizes our government's ability to assess the damage and work on solutions.

And President Trump is wreaking havoc on our critical communication infrastructure with his destructive tariffs.

Rather than boosting U.S. companies, Trump's tariffs have driven up costs and damaged supply chains at exactly the wrong time.

Meanwhile, Democrats have been working diligently to increase network safety and protect Americans' information.

As co-author of the Secure and Trusted Communications Networks Act, I have been a staunch advocate of securing our network supply chain.

Last Congress, we secured the last $3 billion to fully fund the Rip and Replace program and remove vulnerable Chinese equipment from our telecommunications infrastructure. I urge our agencies to ensure smooth and timely completion of this national security imperative.

I have been dedicated to advancing innovations such as open radio access networks, or Open RAN, to bolster our supply chain diversity.

And earlier this week, my bill, the FUTURE Networks Act, passed the House. This bill would bring the brightest minds across industry, academia, and the government to collaborate on the development of our next generation wireless technologies. Including identifying supply chain and cybersecurity vulnerabilities, so that we can more effectively prevent them.

These are important steps to strengthen network security. And we must build on this work, as America faces growing cyberthreats.

This is not the time for inaction. I urge my Republican colleagues to speak up and hold the Trump administration accountable for security failures.

We must work on bipartisan solutions to secure our communications networks, as our Subcommittee has historically done.

I look forward to hearing from our witnesses on how we can proactively protect against future attacks.

And with that, I yield the balance of my time…