Senator Cantwell Opening Statement and Q&A
Subcommittee on Telecommunications and Media Hearing
"Signal Under Siege: Defending America's Communications Networks"
Tuesday, December 2, 2025
[VIDEO]

Sen. Cantwell: Madam Chair, thank you so much for holding this hearing, to you and to Ranking Member Luján.

I want to focus on Salt Typhoon, obviously. The Chinese government's espionage operation deeply penetrated networks of at least nine U.S. telecom companies, including AT&T and Verizon. It has been described as the worst telecom hack in our nation's history, and the Chinese government-sponsored hackers broke into our nation's telecommunications backbone. They exploited the wiretapping system that our law enforcement agencies rely on under the Communications Assistance for Law Enforcement Act -- known as CALEA.

These systems became an open door for Chinese intelligence. Salt Typhoon allowed the Chinese operation to track millions of Americans' locations in real time, record phone calls at will and read our text messages. Their targets included then-candidates President Trump and Vice President Vance, as well as senior government officials. And the hackers were also able to determine who the U.S. Government was wiretapping, including suspected Chinese spies, telling Beijing which of their operatives might be compromised.

So how did this happen? Senior national security officials said the breach occurred in large part because telecommunications companies failed to implement rudimentary – rudimentary! -- cybersecurity measures. Investigators found legacy equipment not updated in years, router vulnerabilities with patches available for seven years -- seven years! -- that were never applied, and hackers acquiring credentials through weak passwords.

Security professionals across the industry were shocked because this kind of basic failure would not be acceptable in health care or banking or in technology firms. Yet here we are: the telecom system -- basically the most sensitive communications [were compromised]. AT&T and Verizon claimed they contained the attack, but government officials and cybersecurity experts remain deeply skeptical. The FBI said it cannot predict when we will have a "full eviction" of these bad actors, and even Chairman Carr acknowledged when he was rolling back the rules that protected [Americans], "We are still being exploited."

Earlier this year, I wrote to the CEOs of AT&T and Verizon, demanding that they provide documentation of their remedies. Both companies refused -- hardly a transparent effort. I believe that the American people deserve to know whether China is still inside our telecom networks. We deserve to know.

Perhaps the most telling response in the breach came from the FBI itself. In an unprecedented step, last December, the FBI and CISA urged all Americans to use encrypted messaging -- basically apps like Signal -- to protect their communications. Hmm…interesting, "Encryption is your friend," they said. Think about that. Our federal law enforcement agencies are telling Americans, "You cannot trust the security of your own telephone networks." That's what they're saying, and "you should use encrypted communication."

So, Ms. Jordan, what level of requirements should we be putting on our wireless providers that make sure that we are getting the level of security that Americans deserve? And when we're handing them over such

valuable resources like spectrum, and they are trying to constantly end-run important national security and DoD initiatives just to get their hands on the spectrum, what requirements should we be putting in place that really do make Americans more secure in their communications?

Ms. Jordan: There must be structured cybersecurity requirements levied. I'm not talking about a checklist -- which has been referred to -- but cyber risk management planning and executing those plans. That has to be put in place, and it should be a requirement. The FCC has already required it of certain…subsections of the communications sector. In fact, in August, this administration proposed it for subsea cable licensees. So continuing along that path -- the continued partnership of industry, the telecommunications industry, with government, the intelligence sector, CISA, others who know of the recent threats. And as you mentioned, doing basic cyber hygiene. You know, I would never let my iPhone go seven years without a patch update, right? Ordering a pizza sometimes requires two-factor authentication. Why are our providers not implementing basic hygiene? They should be held accountable, and they should be doing a structured plan, and they're being held to a verification regime that would give you the information that you asked for and didn't receive.

Sen. Cantwell: Well, what about the FCC? Walking back requirements…it's like they're supposed to be the overall entity that says, look, here's how you have these communications licenses to provide communication, yet if you're not going to do good hygiene, why should we keep your license?

Ms. Jordan: Yes, I don't believe that a fallback of enforcement action is appropriate, because that's after the fact. So again, they should be leveraging this requirement to use the cybersecurity framework, or something similar, to do structured planning and execution of cyber risk management across the entire communications sector. They shouldn't be doing it in little pieces like the E-ACAM or the sub cable or this packet. It should be done pervasively.

Sen. Cantwell: Well, the NARUC is a similar organization that does this for the grid itself. Do you think that that's what we need here, something like that, where, at least, there's a dynamic and input? I mean, me personally, I think this is -- we know this is the information age. We know that this is what's going to happen. So, letting these guys off the hook when [there is] so much vulnerability for Americans that our FBI and law enforcement are telling us – "use encrypted networks." It's gotten to a point where we've got to do something to better help the public. Why have…basically, you're just setting them up -- you're just setting them up to say, "You are going to be a target."

Ms. Jordan: I agree, and I think that there are some aspects of what China is doing that our nation state, and therefore even the telecom providers, might not be able to stave them off. But if the providers are not doing basic hygiene across their networks consistently, then yes, they should be held accountable. I'm not saying [a] nation state comes in and does something that we couldn't predict. That's a different scenario. But they should be held accountable to doing the basic hygiene -- patching, not default passwords, encryption, those kinds of things.

Sen. Cantwell: Well, I think that's the most shocking thing. And this Committee has had several hearings, and there was another big break [in], and that was exactly the same issue. There was a patch--it was available. You know, as we've looked at privacy laws and what you need to do if you're providing some sort of [security] system? Nothing against 20 or 21-year-old administrators, but you've got to have more hierarchy to your enforcement and capabilities on security than just hiring a bunch of very smart, talented people when you have consumers who are going to be vulnerable to these kinds of things. So, we look forward to working with the Subcommittee, Madam Chair, and figuring out what we can do to better protect Americans. Thank you.

###