Testimony of Debra Jordan
Former Chief, Public Safety and Homeland Security Bureau
Federal Communications Commission
Before the
Subcommittee on Telecommunications and Media
Committee on Commerce, Science, and Transportation
United States Senate

"Signal Under Siege: Defending America's Communications Networks"
December 2, 2025

Good morning, Chair Fischer, Ranking Member Luján, Chair Cruz, Ranking Member Cantwell, and Members of the Subcommittee. Thank you for the opportunity to appear before you today.

I appreciate the Senate's interest in this critical and urgent topic and am honored to share my perspective on Defending America's Networks. I'm grateful to have served for nearly 10 years at the Federal Communications Commission as the Deputy and then Bureau Chief for the Public Safety & Homeland Security Bureau, where my responsibilities included national security, cybersecurity, and resilience of the communications sector. As a career civil servant, I was honored to have served under four Commission Chairs, from both parties. My responsibilities included interagency and multi-stakeholder engagements regarding the communications sector and its impacts on our nation either directly or through cascading effects on other critical infrastructure sectors – such as electric, water, transportation, and healthcare.

Before joining the FCC, I spent three decades as a civilian with the U.S. Navy, serving as Command Information Officer for Naval Facilities and Engineering Command. There, I developed and obtained funding to implement the Navy's first ever cybersecurity framework for critical systems such as electrical, water, and wastewater.

A little over a year ago, while I was at the FCC, the U.S. uncovered Salt Typhoon, a sophisticated campaign sponsored by the Chinese government. We know now they infiltrated nine of our nation's largest communications providers, and at least 200 other U.S. organizations, including government agencies. Believed to have been carried out by an advance persistent threat actor attributed to the Chinese Ministry of State Security (MSS), Salt Typhoon exfiltrated millions of metadata records and content associated with calls and text messages of targeted individuals to include then-candidates President Trump and Vice President Vance, then Vice President Harris, and members of Congress. To be specific:

- They monitored live phone calls, gaining access to cellphone and data networks, enabling real-time eavesdropping of calls and texts.

- They harvested sensitive data by collecting private communications, including those of individuals involved in government or political activities
- And they compromised law enforcement systems by accessing systems that log U.S. law enforcement requests for criminal wiretaps, potentially tipping off Chinese intelligence about American investigative targets.

If that doesn't make you shudder - let's go a little further back in time. Active since at least 2021 but not revealed until much later – is Volt Typhoon. The Volt Typhoon attack was attributed to Chinese hackers who gained wide-spread access to critical infrastructure systems using a tactic known as "living-off-the-land." These hackers stole credentials and quietly used administrative accounts to collect data and retain high level access to essential networks, remaining in the networks in preparation for a potential armed conflict – such as one between the U.S. and China over Taiwan.

This was an earlier advance persistent threat attributed to China. How did it work? Chinese-attributed hackers gained access to numerous critical infrastructure networks and systems with privileged admin-level accounts and valid passwords. They didn't use a virus – but rather gained access through stolen credentials and therefore look like valid users. Basically – living in our networks. They have been quietly using these accounts to:
(1) collect data, including credentials from local and network systems,
(2) put the data into an archive file to stage it for exfiltration, and then
(3) use the stolen valid credentials to maintain persistence.

These attacks highlight the vulnerabilities in our communications networks, which provide the foundation for 1/6 of our nation's economy. And trillions of dollars of economic activity depend on these networks every day. So, how do we secure our communications networks – which serve as the underpinnings of our modern digital society? We can either sit back or lean forward regarding the security of our networks. We can lean forward leveraging flexible cyber standards to support our nation's economy and security, or we can sit back and wait for the inevitable next attack to happen.

After the revelation of Salt Typhoon, the FCC leaned forward in January 2025, by adopting a Declaratory Ruling finding that Section 105 of the Communications Assistance for Law Enforcement Act ("CALEA") requires telecommunications carriers to secure their networks against unlawful access or interception of communications. That action was accompanied by a proposal to require communications service providers to certify to the FCC that they have created and implemented an up-to-date cybersecurity risk management plan, which would strengthen network defenses from future cyberattacks. Similar requirements had already been adopted or proposed in multiple regulatory actions, such as being required of recipients of universal service high-cost support through the Enhanced Alternative Connect America Cost Model. The specific requirements were carefully designed to provide a risk-based, flexible approach while offering the Department of Commerce's National Institute for Standards and Technology (NIST) cybersecurity framework as a recommended option to meet the requirements. This approach was also coordinated with other regulators through the Cybersecurity Forum for Independent and Executive Branch Regulators. It provides a non-prescriptive, risk-based approach that allows agile flexibility, while providing a foundational framework with which to collaborate in a multi-stakeholder environment.

However, on November 20, 2025, the Commission reversed the ruling and putting the nation at risk. The FCC cited engagement with providers and "their agreement to take extensive steps to protect national security interests." However, the Commission does not cite any process by which providers will be held accountable to meet specific commitments. From my experience as Bureau Chief, I am not convinced that providers will take sufficient, sustained actions in the wake of Salt and Volt Typhoon without a strong verification regime. In my experience, the Commission could have incorporated the discussions and agreements from providers into the requirement to create, update, and implement a cyber risk management plan. That would have merged the accountability aspect with the providers' agreements. As things stand now, we can only hope that providers are taking appropriate steps and that these actions are sustained as the cyber threats evolve. And hope is not a strategy to secure our networks.

So, what can Congress do? I have three recommendations:

First, we have tools such as the Cybersecurity Framework developed by NIST. Congress should encourage the FCC to require the NIST Cybersecurity Framework (or similar guidance) for all telecommunications providers. The framework is flexible and developed in collaboration with industry and the public to assist organizations to manage and reduce cyber risks. The FCC already requires small subsets of communications providers to develop and implement cyber risk management plans, citing the NIST Cybersecurity Framework as a model framework; in fact, they just proposed in August to require this of subsea cable licensees. Why not make this a requirement across all communications providers to ensure a ubiquitous level of cyber risk management?

Second, is to upgrade our communications infrastructure. Keeping communications infrastructure current is critical, but also costly. I encourage Congress to fully fund communications infrastructure such as Next Generation 911 and cyber funding for state, local, Tribal, and territorial entities. We can't enable modern digital network security when running on old analog infrastructure.

And lastly, verification must be part of trust. I agree that it's critical for industry to own the implementation of cyber risk management and that collaboration among government and industry stakeholders is key. But trust without verify is an incomplete solution. We must establish a verification regime to ensure the security of our nation's communications infrastructure from the largest to the smallest providers. We've seen time and again through outage and enforcement investigations, where providers have not implemented even some of the most basic cyber hygiene uniformly across their networks, such as changing default passwords. Their networks are large, complex and difficult to secure –

and yet they are critical to our nation’s economy and security. Industry says they’re committed to implementing extensive cyber protections, so let’s establish a regime in a secure setting for them to share their progress and further plans.

Thank you and I look forward to your questions.