STATEMENT OF COMMISSIONER ANNA M. GOMEZ

Re: *Protecting the Nation's Communications Systems from Cybersecurity Threats*, PS Docket No. 22-329, Order on Reconsideration (November 20, 2025).

Salt Typhoon has been described as the worst telecommunications hack in our nation's history. It was a highly coordinated breach of American telecommunications infrastructure carried out by a foreign adversary that targeted American infrastructure, American companies, and American citizens, including the current President of the United States. But more importantly, it was a wake-up call. It showed us just how few incentives exist to force companies to address the vulnerabilities that allowed that attack to happen. And it proves to us that adversaries like the Chinese Communist Party (CCP) will not hesitate to act aggressively and decisively. And neither should we.

Sadly, the Commission today reverses the only meaningful effort this agency has advanced in response to that attack. The January Declaratory Ruling and Notice of Proposed Rulemaking were adopted because immediate action was needed at that time. They sought to create accountability, establish clear cybersecurity obligations, and put in place an enforceable framework to harden networks before the next breach. By rescinding those efforts and offering nothing in their place, the FCC leaves the country less safe at the very moment when these threats are increasing.

We're told the answer is not regulation, but voluntary collaboration. Collaboration is valuable and I support it as one part of a comprehensive cybersecurity strategy. However, collaboration is not a substitute for obligation. Handshake agreements without teeth will not stop state-sponsored hackers in their quest to infiltrate our networks. They won't prevent the next breach. They do not ensure that the weakest link in the chain is strengthened. If voluntary cooperation were enough, we would not be sitting here today in the wake of Salt Typhoon.

To be clear, partnership and collaboration are worthy goals. However, partnership and collaboration that carry no enforceable accountability are insufficient by design. Simply trusting industry to police itself is an invitation for the next breach. And when the next breach occurs, there will be no standards to measure compliance and no mechanism for determining which safeguards should have been in place. That is governing by hope rather than by duty, and the American public deserves better.

I will admit that going over this item was difficult. It read like a one-sided opposing statement, full of bombastic and unproven claims, rather than a level-headed approach to national security. But I found it curious that in it the FCC lists cybersecurity requirements that carriers already face under securities law, under state law, and in unrelated FCC rulemakings. To me, that list proves two points. First, this agency already accepts that requirements are sometimes necessary. Second, those requirements did not address the vulnerabilities that Salt Typhoon exploited. None of the actions cited in this item, like our work to secure undersea cables or the creation of an internal national security brainstorming group, would have prevented that attack. And nothing in this item would prevent the next one.

And the problem does not stop there. Ten months into this Administration, this FCC has still not put forward a single actionable solution to address the growing cybersecurity threat to our communications networks. Not one concrete proposal. Not one protection standard. Not one accountability mechanism. Today's decision is not a cybersecurity strategy. It is a hope and a dream.

This FCC also criticizes the Declaratory Ruling for not specifying which vulnerabilities should be prioritized, and for moving forward with what it calls a "partisan approach" that did not seek public input. If clarity and process were truly the concerns, then the solution should have been to strengthen the item through notice-and-comment and to provide companies with that clarity, not to discard the effort altogether. That is exactly why I proposed a bipartisan rulemaking process that would refine and perfect these requirements. That request, which would have continued this agency's bipartisan tradition of

working together on national security issues, was declined.

Perhaps most concerning of all, the majority bases its decision on the assertion that the previous FCC action was unlawful. That is a statutory interpretation that does not stand to scrutiny. CALEA requires carriers to CALEA requires carriers to "ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with… lawful authorization."[1] That provision therefore places an affirmative cybersecurity obligation on carriers, and the Communications Act gives the FCC authority to implement that obligation. In fact, I have noticed that many of the things the other side disagrees with tend to be simply labeled as "unlawful." Our recently upheld data breach notification rules are one clear example. You may disagree with the policy choice, but that disagreement does not erase that statutory authority. And I worry that this capricious attempt to label this tool as unlawful will hamstring this agency when it is inevitably called upon to respond to the next hack.

But rather than prepare this agency for that scenario, the Commission instead places its blind faith in a new collaborative approach. Yet this FCC does not explain what the approach is, what objectives it will pursue, what milestones it will track, or how the public will know whether it has succeeded. We are told that this internal council will help facilitate coordination, but the item does not describe how the council will translate its work into concrete steps to protect our telecommunications networks. This country cannot afford to wait for slow and cooperative progress that may never materialize.

That choice carries serious consequences. This FCC today is leaving Americans less protected than they were the day this breach was discovered. Salt Typhoon will not be the last attempt to infiltrate our networks, and without immediate action it will not be the last successful one.

History will remember whether we chose to act in the face of clear and imminent danger. The best time to do that was yesterday. The second-best time is now.

[1] 47 U.S.C. § 1004.