STATEMENT OF
CHAIRMAN BRENDAN CARR

Re: Protecting the Nation's Communications Systems from Cybersecurity Threats, PS Docket No. 22-329

As the U.S. intelligence community has explained, Salt Typhoon—a China-sponsored advanced persistent threat group—infiltrated at least eight U.S. communications companies as part of a massive espionage campaign that affected dozens of countries. But Salt Typhoon was just the latest example in a decades-long history of foreign adversaries launching cyberattacks against our communications networks for both espionage and potential sabotage purposes.

In light of these ongoing risks, the U.S. government and the FCC, in particular, must act. But doing anything just so we can say we did something is not the answer. The FCC must take actions that are both lawful and effective. We have been doing exactly that at the FCC this year.

When I started as Chairman, one of the first actions I took was to stand up a new Council on National Security—a body that is staffed with experts that coordinate both within the FCC and across the intelligence community. We have withdrawn recognition for "bad labs" from our equipment authorization program for the first time. We have closed longstanding loopholes in our equipment security rules. We have adopted new security measures for submarine cables. And earlier this month, an FCC delegation traveled to London for a convening of Five Eyes telecom regulators to further our coordination on network security issues.

We have taken many more actions as well. Relevant to today's vote, the FCC has worked directly with carriers who have agreed to make extensive, coordinated efforts to harden their networks against a range of cyber intrusions. These have included accelerated patching of outdated or vulnerable equipment, updating and reviewing access controls, disabling unnecessary outbound connections, improving their threat-hunting efforts, and increasing cybersecurity information sharing.

All of these actions have been well within FCC legal authority and have effectively mitigated network vulnerabilities. In contrast, the Declaratory Ruling that we reconsider today was neither lawful nor effective.

It was unlawful because the FCC purported to read a statute that required telecommunications carriers to allow lawful wiretaps within a certain portion of their network as a provision that required carriers to adopt specific network management practices in every portion of their network. It was ineffective because it neither responded to the nature of the relevant cybersecurity threats nor was it consistent with the agile and collaborative approach to cybersecurity that has proven successful.

Indeed, when the prior Commission hastily rushed the item out the door just days before the presidential transition I said the following: "no[t] one official in the intelligence community has encouraged me to vote in favor of this FCC action. In fact, I was told that this type of FCC regulatory action at this moment would be counterproductive and deter the productive collaboration that is necessary today." Let me just reemphasize that here today. Biden-era cyber officials said at the time that the FCC's decision would not be merely ineffective—it would be counterproductive.

For these reasons, the Commission votes today to reverse that rushed and eleventh-hour approach to cybersecurity. In its place, we will continue our work to strengthen and harden the nation's communications networks and infrastructure.

For their great work on today's item, I want to thank Austin Randazzo, Leon Kenworthy, Scott Bouboulis, Josh Gehret, James Graves, Doug Klein, Hallie Laws, Zoe Li, and Zenji Nakazawa.