FCC NEWS from the Federal Communications Commission

**Media Contact:**
MediaRelations@fcc.gov

**For Immediate Release**

# CHAIRWOMAN ROSENWORCEL ANNOUNCES AGENCY ACTION TO REQUIRE TELECOM CARRIERS TO SECURE THEIR NETWORKS

***Proposes Swift Steps to Strengthen U.S. Communications from Future Cyberattacks***

WASHINGTON, January 16, 2025—Following recent reports involving an intrusion by foreign actors into U.S. communications networks, FCC Chairwoman Jessica Rosenworcel today announced the agency has taken action to safeguard the nation's communications systems from real and present cybersecurity threats, including from state-sponsored cyber actors from the People's Republic of China.

**Federal Communications Commission Chairwoman Jessica Rosenworcel:** "In response to Salt Typhoon, there has been a government-wide effort to understand the nature and extent of this breach, what needs to happen to rid this exposure in our networks, and the steps required to ensure it never happens again. At the Federal Communications Commission, we now have a choice to make. We can turn the other way and hope this threat goes away. But hope is not a plan. Leaving old policies in place when we know what new risks look like is not smart. Today, in light of the vulnerabilities exposed by Salt Typhoon, we need to take action to secure our networks. Our existing rules are not modern. It is time we update them to reflect current threats so that we have a fighting chance to ensure that state-sponsored cyberattacks do not succeed. The time to take this action is now. We do not have the luxury of waiting. Telecommunications networks are essential for everything in day-to-day life, from our national defense to public safety to economic growth. The actions we take and propose here will strengthen our cybersecurity safeguards and enhance our resilience against future attacks."

**National Security Advisor Jake Sullivan:** "The FCC's Declaratory Ruling and Notice of Proposed Rulemaking is a critical step to require U.S. telecoms to improve cybersecurity to meet today's nation state threats, including those from China's well-resourced and sophisticated offensive cyber program."

**Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly:** "The FCC's actions today are an important step in securing the nation's telecommunications infrastructure against the very real threat posed by the PRC and other threat actors. CISA will continue to work with all critical infrastructure entities to implement measures that help them safeguard their networks."

The Commission adopted a Declaratory Ruling finding that section 105 of Communications Assistance for Law Enforcement Act ("CALEA") affirmatively requires telecommunications carriers to secure their networks from unlawful access or interception of communications. That action is accompanied by a proposal to require communications service providers to submit an annual certification to the FCC attesting that they have created, updated, and implemented a

cybersecurity risk management plan, which would strengthen communications from future cyberattacks.

The Declaratory Ruling takes effect immediately. The Notice of Proposed Rulemaking invites comment on cybersecurity risk management requirements for a wide range of communications providers. The Notice also seeks comment on additional ways to strengthen the cybersecurity posture of communications systems and services.

In November, the Commission proposed cybersecurity risk management plan requirements for submarine cable landing applicants and licensees. In addition, the Commission previously proposed that participants in the Emergency Alert System and Wireless Emergency Alerts maintain cybersecurity risk management plans.

###