United States Senate
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
WASHINGTON, DC 20510–6125
WEBSITE: https://commerce.senate.gov

November 18, 2025

Brendan Carr
Chairman
Federal Communications Commission
45 L Street, NE
Washington, DC 20554

Dear Chairman Carr:

I write in strong opposition to your effort to roll back the Federal Communications Commission's (FCC) ruling to secure telecommunications networks specifically put into place after last year's Chinese-state-sponsored Salt Typhoon incursion—one of the worst cyberattacks in history.[1] With these highly sophisticated foreign threat actors, our efforts should be focused on further enhancing the cybersecurity of our critical infrastructure networks, not rolling back existing protections.

U.S. officials have said that Salt Typhoon allowed the Chinese government to "geolocate millions of individuals," "record phone calls at will," and included almost every American.[2] Their specific targets included then-candidates President Trump and Vice President J.D. Vance.[3] This year, the FBI confirmed that the hackers accessed and copied select information on wiretap systems used by U.S. law enforcement.[4] Experts agree that the attack has not been fully remediated from telecommunications networks, and your own draft ruling concedes that vulnerabilities "are still being exploited."[5]

[1] See, e.g., David Jones, Salt Typhoon telecom hacks one of the most consequential campaigns against US ever, expert says, *Cybersecurity Dive* (May 1, 2025), https://www.cybersecuritydive.com/news/salt-typhoon-telecomhacks-one-of-the-most-consequential-campaigns-against/746870.
[2] A.J. Vicens, US adds 9th telecom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage, *Reuters* (Dec. 27, 2024), https://www.reuters.com/technology/cybersecurity/us-adds-9th-telcom-list-companieshacked-by-chinese-backed-salt-typhoon-2024-12-27/; Adam Goldman, 'Unrestrained' Chinese Cyberattackers May Have Stolen Data From Almost Every American, *New York Times* (Sept. 4, 2025) https://www.nytimes.com/2025/09/04/world/asia/china-hack-salt-typhoon.html/
[3] Devlin Barrett, et al., Chinese Hackers Are Said to Have Targeted Phones Used by Trump and Vance, *New York Times* (Oct. 25, 2024), https://www.nytimes.com/2024/10/25/us/politics/trump-vance-hack.html.
[4] Federal Bureau of Investigation, FBI Seeking Tips about PRC-Targeting of US Telecommunications (Apr. 24, 2025), https://www.ic3.gov/PSA/2025/PSA250424-2.
[5] David DiMolfetta, FBI awaits signal that Salt Typhoon is fully excised from telecom firms, official says, NextGov (May 1, 2025); https://www.nextgov.com/cybersecurity/2025/05/fbi-awaits-signal-salt-typhoon-fully-excised-telecom-firms-official-says/404982/; FCC-CIRC 2511-04 at para. 29.

On June 12, 2025, I wrote to the CEOs of Verizon and AT&T demanding that they provide documentation of remediating the Salt Typhoon exploits that deeply penetrated their networks, but they have failed to do so.[6] Since then, U.S. law enforcement and intelligence agencies warned the Salt Typhoon espionage campaign is far more sweeping than originally believed, hacking at least 200 U.S. organizations and 80 countries.[7] The FBI, Cybersecurity and Infrastructure Security Agency, the National Security Agency, our close Five Eyes allies, and agencies from Japan and other European countries issued a joint cybersecurity advisory that Salt Typhoon was "targeting networks globally" such as "telecommunications, government, transportation, lodging, and military infrastructure networks."[8] The advisory also noted that while the focus was on "routers of major telecommunications providers," the hackers also "leverage compromised devices and trusted connections to pivot into other networks."[9]

In January 2025, and in response to Salt Typhoon, the Federal Communications Commission ruled that the Communications Assistance for Law Enforcement Act (CALEA) "affirmatively requires telecommunications carriers to secure their networks from unlawful access or interception of communications."[10] This simply brought the agency's interpretation of the statute in line with current network realities. This step was one of the first updates to the FCC's implementation of CALEA in decades and a commonsense acknowledgement that providers are responsible for protecting public safety against cybersecurity threats.

You have now proposed to reverse this requirement after heavy lobbying from the very telecommunications carriers whose networks were breached by Chinese hackers.[11] Your proposal to rescind this ruling would undermine the FCC's ability to hold carriers accountable for protecting our nation's critical communications infrastructure. And you propose to replace the ruling with no action whatsoever, instead relying on "collaboration" with carriers who failed to detect the hacks and have not provided me any of the evidence I requested that they have removed the intruders from their networks. Your order to rescind the January ruling also claims without evidence that the "collaborative approach to cybersecurity continues to be effective."[12]

I am concerned that your move to drop cybersecurity requirements on carriers is part of a pattern of weakness on national security issues. In 2024, you opposed the prior FCC's efforts to block Chinese companies from providing internet service in this country, claiming that the FCC lacked

---

[6] https://www.commerce.senate.gov/2025/6/cantwell-demands-answers-from-at-t-and-verizon-on-chinese-salt-typhoon-hack.
[7] Joseph Menn, FBI warns Chinese hacking campaign has expanded, reaching 80 countries, *Washington Post* (Aug. 27, 2025), https://www.washingtonpost.com/technology/2025/08/27/fbi-advisory-china-hacking-expansion/
[8] Joint Cybersecurity Advisory, Sept. 2025, https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF.
[9] *Id.*
[10] Protecting the Nation's Communications Systems from Cybersecurity Threats, Declaratory Ruling and Notice of Proposed Rulemaking, FCC 25-9.
[11] *See* Petition for Reconsideration of CTIA – The Wireless Association, NCTA – The Internet & Television Association, and USTelecom – The Broadband Association, (Feb. 18, 2025); Reply in Support of Petition for Reconsideration by CTIA, NCTA, and USTelecom, (Mar. 7, 2025); CTIA, NCTA, and USTelecom Ex Parte Letter (July 25, 2025); CTIA, NCTA, and USTelecom Ex Parte Letter (Aug. 4, 2025); CTIA, NCTA, and USTelecom Ex Parte Letter (Sept. 5, 2025); CTIA et al. Ex Parte Letter (Sept. 10, 2025); CTIA et al. Ex Parte (Oct. 16, 2025).
[12] FCC-CIRC 2511-04.

authority to do so. And after helping lead the movement during the Biden administration to require that TikTok divest of Chinese influence, you have been silent while the Trump administration ignored the law and threatens to leave TikTok's algorithm under Chinese control. You also stood by while Republicans in Congress passed a law that threatens national security with rash plans to reallocate spectrum used for defense and public safety.

These national security concerns also demonstrate why it is vital that you testify before this Committee to explain how you can fulfill your duty to promote the "national defense" as Chair of the FCC.[13]

I strongly encourage that you reverse course, withdraw the draft ruling, and maintain the FCC's ruling that the telecommunications companies are required by the law to secure their networks from unlawful access or interception of communications.

The Senate Committee on Commerce, Science, and Transportation has direct oversight and legislative jurisdiction over the FCC. Please provide the following documents and information no later than November 25, 2025:

1. A copy of any cybersecurity assessment the FCC conducted before moving to repeal its prior ruling. Please provide any documents.
2. Any documents the telecommunications companies shared with you that support their claims that they removed Salt Typhoon hackers from their networks, including, but not limited to, Mandiant digital forensic reports.
3. Documents and information sufficient to demonstrate the FCC's collaborative approach to cybersecurity with telecommunications providers "continues to be effective."

To the extent any of the requested materials contain classified information, please segregate any such information and contact my staff to coordinate production with the Office of Senate Security. Thank you for your attention to this important matter.

Sincerely,

Maria Cantwell
United States Senator
Ranking Member, Committee
on Commerce, Science, and
Transportation

[13] 47 U.S.C. Sec. 151.