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

February 3, 2026

Mr. Chairman:

I am requesting the Senate Committee on Commerce, Science, and Transportation hold an oversight hearing with the CEOs of AT&T and Verizon to examine the security of their telecommunications networks following the deep penetration by Chinese state-sponsored hackers "Salt Typhoon"—widely regarded as one of the worst cyberattacks in our nation's history.[1] For months, I have sought specific documentation from AT&T and Verizon that would purportedly corroborate their claims that their networks are now secure from this attack.[2] Unfortunately, both AT&T and Verizon have chosen not to cooperate, which raises serious questions about the extent to which Americans who use these networks remain exposed to unacceptable risk. Since then, expert witnesses warned this Committee about the ongoing security risks posed by Salt Typhoon,[3] while reports indicate that Salt Typhoon hackers are likely still inside U.S. telecommunications networks[4] and may have even breached email accounts used by congressional staff.[5] Given these mounting concerns, I believe we must hear directly from the CEOs of AT&T and Verizon so Americans have clarity and confidence about the security of their communications.

In the past several months, we learned that the scope of the Salt Typhoon attack was greater than previously believed. According to the Federal Bureau of Investigations (FBI), the Salt Typhoon hackers targeted more than 200 U.S. organizations and 80 countries[6]—allowing Chinese intelligence officers to potentially surveil Americans' private communications abroad and use

---

[1] Goldman, Adam, "'Unrestrained' Chinese Cyberattackers May Have Stolen Data from Almost Every American", *The New York Times,* (Sep. 4, 2025); https://www.nytimes.com/2025/09/04/world/asia/china-hack-salt-typhoon.html; *see also* Surbhi Misra and David Shepardson, "AT&T, Verizon targeted by Salt Typhoon cyberespionage operation, but networks secure", *Reuters,* (Dec. 29, 2024); https://www.reuters.com/technology/cybersecurity/chinese-salt-typhoon-cyberespionage-targets-att-networks-secure-carrier-says-2024-12-29/.

[2] *See* Press Release, "Cantwell Demands Answers from AT&T and Verizon on Chinese 'Salt Typhoon' Hack", *U.S. Senate Committee on Commerce, Science, and Transportation,* (Jun. 12, 2025); https://www.commerce.senate.gov/2025/6/cantwell-demands-answers-from-at-t-and-verizon-on-chinese-salt-typhoon-hack.

[3] Hearing, "Signal Under Siege: Defending America's Communications Networks", *U.S. Senate Committee on Commerce, Science, and Transportation,* (Dec. 2, 2025); https://plus.cq.com/doc/congressionaltranscripts-8361130?4.

[4] Miller, Maggie, "Warner cautions that Chinese hacker are likely still in US telecom networks", *Poltico Pro,* (Dec. 12, 2025); https://subscriber.politicopro.com/article/2025/12/warner-cautions-that-chinese-hackers-are-likely-still-in-us-telecom-networks-00689608?site=pro&prod=alert&prodname=alertmail&linktype=article&source=email.

[5] Sevastopulo, Demetri, "China hacked email systems of US congressional committee staff", *Financial Times,* (Jan. 7, 2026); https://www.ft.com/content/44f730c4-7de3-4a09-88dd-41ea9c373dcb?FTCamp=engage/CAPI/desktopapp/Channel_Bloomberg//B2B.

[6] Menn, Joseph, "FBI warns Chinese hacking campaign has expanded, reaching 80 countries", *The Washington Post,* (Aug. 27, 2025); https://www.washingtonpost.com/technology/2025/08/27/fbi-advisory-china-hacking-expansion/.

their cellphone geolocation data to track their movements across the globe.[7] In August 2025, the FBI's top cyber official, Assistant Director Brett Leatherman, called Salt Typhoon "one of the more consequential cyber espionage breaches we have seen here in the United States."[8] The FBI and other federal agencies have urged Americans to use only encrypted messaging applications due to vulnerabilities from Salt Typhoon.[9] In September 2025, a Joint Cybersecurity Advisory issued by a collection of U.S. and international intelligence and cybersecurity agencies warned that Chinese state-sponsored cyber threat actors, including Salt Typhoon, target "large backbone routers of major telecommunications providers" like AT&T and Verizon and then "modify routers to maintain persistent, long-term access to networks."[10]

The agencies detailed guidance on how to mitigate the risk from Advanced Persistent Threat actors like Salt Typhoon and urged potential targets like telecommunications providers to "hunt for malicious activity and to apply the mitigations" called for in the Advisory.[11] However, reports indicate the telecommunications providers have taken few protective actions thus far due to the costs involved in securing their networks while experts have expressed skepticism that industry is taking the necessary mitigation steps.[12] For example, in December the former Chief of the Federal Communications Commission's Public Safety and Homeland Security Bureau testified before the Telecommunications Subcommittee, "I'm not convinced that providers will take sufficient and sustained actions in the wake of Volt and Salt Typhoon without a strong verification regime" and further stated: "if the providers are not doing basic hygiene across their networks consistently, then yes, they should be held accountable."[13] I agree.

That is why I sent letters to AT&T CEO John Stankey and then-Verizon CEO Hans Vestberg requesting documents and information that would shed light on the actions they took to secure their networks following the Salt Typhoon attack and help Congress evaluate the current security risks posed to the 265 million Americans who use their services.[14] In response, both companies confirmed the existence of security assessments conducted by Mandiant, a digital forensics and incident response provider, that would presumably document the vulnerabilities identified and detail what corrective actions the telecommunications providers need to take to protect

---

[7] Viswanatha, Aruna, and Sarah Krouse, "Chinese Spies Hit More Than 80 Countries in 'Salt Typhoon' Breach, FBI Reveals", *The Wall Street Journal,* (Aug. 27, 2025); https://www.wsj.com/politics/national-security/chinese-spies-hit-more-than-80-countries-in-salt-typhoon-breach-fbi-reveals; *see also* Cybersecurity Advisory, "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System", *Cybersecurity and Infrastructure Security Agency,* (Sep. 30, 2025); https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a.

[8] *Id.*

[9] Doffman, Zak, "FBI Warns iPhone and Android Users—Stop Sending Texts", *Forbes,* (Dec. 6, 2024); https://www.forbes.com/sites/zakdoffman/2024/12/06/fbi-warns-iphone-and-android-users-stop-sending-texts/?streamIndex=0.

[10] Joint Cybersecurity Advisory, "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System", *National Security Agency, et. al.,* (Sep. 2025); https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF

[11] *Id.*

[12] *See supra* n. 5, *see also* Johnson, Derek B., "The Congressional remedy for Salt Typhoon? More information sharing with industry", *Cyberscoop,* (Dec. 2, 2025); https://cyberscoop.com/salt-typhoon-senate-commerce-hearing-fcc-telecom-cybersecurity/.

[13] *See supra* n. 3

[14] *See supra* n. 2

Americans' privacy and security.[15] However, both AT&T and Verizon have refused to make these key reports available without any compelling reason to keep them hidden from Congress.

As a result, I wrote to Mandiant requesting copies of these reports and other relevant documentation. But AT&T and Verizon apparently intervened to block Mandiant from cooperating with my requests.[16] I believe this course of engagement raises serious questions about AT&T's and Verizon's current security posture, as they are either unwilling or unable to provide specific documentation that would show their networks are secure.

If AT&T and Verizon are not going to provide Congress key documentation voluntarily, then I believe this Committee must promptly convene a hearing with their CEOs so they can explain why Americans should have confidence in the security of their networks amid mounting evidence that the Salt Typhoon hackers remain active and undeterred. The American public deserves transparency and certainty that our nation's major telecommunications networks are not currently exposed to unacceptable risks. This oversight hearing would be an opportunity to provide precisely that.

Sincerely,

Maria Cantwell
Ranking Member

[15] Letter to Ranking Member Maria Cantwell from Michael Ferguson, Executive Vice President for Federal Legislative Relations at AT&T, (Jun. 26, 2025); on file with Democratic Committee Staff; *see also* Meeting between Democratic Committee staff and Verizon, (Jun. 17, 2025); *see also* Letter to Ranking Member Maria Cantwell, from Robert S. Fisher, Senior Vice President for Federal Government Relations and Public Affairs at Verizon, (Jul. 3, 2025); on file with Democratic Committee Staff.

[16] Letter to Ranking Member Maria Cantwell from Anne Wall, Head of U.S. Federal Government Affairs and Public Policy at Mandiant, (Aug. 6, 2025); on file with Democratic Committee Staff. AT&T and Verizon apparently intervened to claim attorney-client privilege over these Mandiant reports—despite the fact that neither company previously asserted any such privilege when asked by my staff. In any event, as you have recognized, Congress is not bound by common law privileges. *See, e.g.*, Letter to Vic Sher and Matt Edling, of Sher Edling L.L.P., (Sep. 25, 2023); https://www.commerce.senate.gov/services/files/2781AC16-2206-49C7-85BE-D74B27306929.