TED CRUZ, TEXAS, CHAIRMAN

JOHN THUNE, SOUTH DAKOTA
ROGER F. WICKER, MISSISSIPPI
DEB FISCHER, NEBRASKA
JERRY MORAN, KANSAS
DAN SULLIVAN, ALASKA
MARSHA BLACKBURN, TENNESSEE
TODD YOUNG, INDIANA
TED BUDD, NORTH CAROLINA
ERIC SCHMITT, MISSOURI
JOHN CURTIS, UTAH
BERNIE MORENO, OHIO
TIM SHEEHY, MONTANA
SHELLEY MOORE CAPITO, WEST VIRGINIA
CYNTHIA M. LUMMIS, WYOMING

MARIA CANTWELL, WASHINGTON
AMY KLOBUCHAR, MINNESOTA
BRIAN SCHATZ, HAWAII
EDWARD J. MARKEY, MASSACHUSETTS
GARY C. PETERS, MICHIGAN
TAMMY BALDWIN, WISCONSIN
TAMMY DUCKWORTH, ILLINOIS
JACKY ROSEN, NEVADA
BEN RAY LUJÁN, NEW MEXICO
JOHN W. HICKENLOOPER, COLORADO
JOHN FETTERMAN, PENNSYLVANIA
ANDY KIM, NEW JERSEY
LISA BLUNT ROCHESTER, DELAWARE

BRAD GRANTZ, MAJORITY STAFF DIRECTOR
LILA HARPER HELMS, DEMOCRATIC STAFF DIRECTOR

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

June 12, 2025

John T. Stankey
Chairman and Chief Executive Officer
AT&T Inc.
208 S. Akard St.
Dallas, TX 75202

Dear Mr. Stankey:

Last year, Chinese state-sponsored hackers widely known as "Salt Typhoon" deeply penetrated major U.S. telecommunications networks including AT&T. Experts have described this as one of the worst cyberattacks in our nation's history.[1] In December 2024, AT&T claimed its network was secure and that there was "no activity by nation-state actors in our networks at this time."[2] However, recent reports indicate broad, ongoing doubts among security experts that Salt Typhoon has been fully eradicated from our telecommunications networks. I am deeply concerned that despite your assurances, the 120 million Americans who use AT&T and the first responders who rely on your FirstNet network remain at serious risk and I am requesting AT&T provide relevant security documents and information.

Current and former government experts continue to indicate that Salt Typhoon may remain active in U.S. networks. They have explained how telecommunications networks are complex and full of hardware and software vulnerabilities Salt Typhoon can exploit to create multiple pathways to reenter the network. Experts also noted the sheer scale of any network would likely need a forensic analysis of tens of thousands of endpoints to identify all potential compromises.[3]

---

[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-telecom-hacks-one-of-the-most-consequential-campaigns-against/746870/. https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/.

[2] 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/.

[3] 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/; Derek B. Johnson, A house full of open windows: Why telecoms may never

Furthermore, weeks before AT&T claimed the attack was resolved, the U.S. government publicly stated that the scope and significance of the compromise in traditional telecommunications networks made it "impossible" for agencies "to predict a time frame on when we'll have a full eviction," and urged Americans to use encrypted voice and text applications to minimize the chances of the hackers intercepting their communications.[4] In December 2024, the Deputy National Security Advisor for Cyber and Emerging Technology stated the "Chinese gained access to networks and essentially had broad and full access," allowing them to "geolocate millions of individuals" and "record phone calls at will."[5] Their targets included prominent U.S. political figures, from Members of Congress to then-candidates President Trump and Vice President J.D. Vance.[6] On April 24, 2025, the FBI confirmed that the hackers also stole call data logs, private communications of certain victims, and accessed and copied select information on wiretap systems used by U.S. law enforcement.[7]

The FBI, NSA, the Cybersecurity and Infrastructure Security Agency, and the Federal Communications Commission have issued guidance and proposed regulations to telecom providers in response to the Salt Typhoon incursion.[8] It is unclear if AT&T has made changes to its policies and practices in accordance with this targeted guidance.

Given the national security, critical infrastructure, and privacy risks involved, AT&T must make every effort to protect their customers against these highly sophisticated foreign adversaries—and be fully transparent about such efforts. Please provide the following documents and information from September 1, 2024, to present no later than June 26, 2025:

1. A copy of AT&T's remediation plan in response to the Salt Typhoon attacks.
2. All threat assessments related to the security risk of nation-state actors hacking AT&T's systems, including but not limited to the FirstNet network.
3. A list of all vulnerabilities AT&T has identified that allowed nation-state actors to gain broad, full access to its networks, and to what extent it has been mitigated or remediated.

---

purge their networks of Salt Typhoon, CyberScoop (May 21, 2025), https://cyberscoop.com/salt-typhoon-chinese-hackers-us-telecom-breach/.

[4] Kevin Collier, U.S. officials urge Americans to use encrypted apps amid unprecedented cyberattack (Dec. 3, 2024), https://www.nbcnews.com/tech/security/us-officials-urge-americans-use-encrypted-apps-cyberattack-rcna182694.

[5] 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-companies-hacked-by-chinese-backed-salt-typhoon-2024-12-27/

[6] 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.

[7] Federal Bureau of Investigation, FBI Seeking Tips about PRC-Targeting of US Telecommunications (Apr. 24, 2025), https://www.ic3.gov/PSA/2025/PSA250424-2.

[8] CISA, Enhanced Visibility and Hardening Guidance for Communications Infrastructure (Dec. 4, 2024), https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure; FCC, Protecting the Nation's Communications Systems from Cybersecurity Threats, FCC 25-9 (Jan. 16, 2025).

4. All documents relating to AT&T's determination that there was no longer activity by nation-state actors in its networks.
5. All records related to the costs and expenses AT&T incurred to secure its networks from nation-state actors and attackers, including but not limited to a third-party audit.
6. All AT&T policies and best practices relating to the encryption of customer data.

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
Ranking Member