July 23, 2025

Sandra Joyce
Executive Vice President
Mandiant Intelligence and Government Affairs
11955 Freedom Drive
Reston, VA 20190

Dear Ms. Joyce:

Last year, the Chinese state-sponsored cyber espionage group known as "Salt Typhoon" hacked major U.S. telecommunications networks including AT&T and Verizon. Experts have widely described this as one of the worst and most consequential national security breaches in our nation's history.[1] In December 2024, AT&T and Verizon both claimed their networks were secure, but only weeks before the companies made those announcements the U.S. government warned the breach was so significant it made it "impossible" for agencies "to predict a time frame on when we'll have a full eviction."[2]

To better understand the basis for AT&T's and Verizon's claims, I sent letters to each company requesting relevant documents and information regarding the actions they took to secure their networks. In response, both companies acknowledged they retained Mandiant to conduct a comprehensive assessment of the cyber incident and verify the extent to which the incident has been contained. Accordingly, I am requesting Mandiant provide relevant documents in its possession that are responsive to my concerns.

Notwithstanding AT&T's and Verizon's December 2024 statements, recent reports indicate broad, ongoing doubts among cybersecurity experts that Salt Typhoon has been fully eradicated

[1] *See, e.g.,* Jones, David, "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/; *see also* Nakashima, Ellen, "Top senator calls Salt Typhoon 'wors telecom hack I our nation's history'", *The Washington Post*, (Nov. 21, 2024); https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/.

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

from our telecommunications networks.[3] According to a June 2025 memo from the Department of Homeland Security, Salt Typhoon "extensively compromised" a state's Army National Guard network last year, collecting its "network configuration and its data traffic with its counterparts' networks in every other US state," including "these networks' administrator credentials and network diagrams—which could be used to facilitate follow-on Salt Typhoon hacks of these units."[4] One cyber CEO and former CIA officer recently warned, "zero chance we've seen the last of Salt Typhoon," while another expert stated "critical infrastructure, whether it's telecommunications, defense or public health, is increasingly vulnerable to advanced, persistent threat actors like Salt Typhoon."[5] And a Cisco report found Salt Typhoon "demonstrated [the threat actor's] ability to persist in target environments… maintaining access in one instance for over three years."[6]

Given the ongoing concerns about the security of our critical networks, on June 12, 2025, I sent letters to AT&T CEO John Stankey and Verizon CEO Hans Vestberg requesting documents and information regarding the extent to which vulnerabilities remain in their networks as a result of Salt Typhoon and the risks this may pose to the 265 million Americans who use their services—including the first responders who rely on AT&T's FirstNet network.[7] The narrow set of documents I sought would help confirm the basis for the companies' public assertions that the Salt Typhoon threat has been contained—information that I believe the Committee deserves in order to properly conduct its oversight. Both AT&T and Verizon confirmed the existence of relevant assessments conducted by Mandiant that are responsive to my letter, but they have thus far refused to make these key reports available without any compelling reason to keep them hidden from Congress.

This response only heightens my concerns about AT&T's and Verizon's current security posture, as they are either unwilling or unable to provide specific documentation that would corroborate their claims that their networks are secure.

---

[3] DiMolfetta, David, "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/; *see also* Johnson, Derek B., "A house full of open windows: Why telecoms may never purge their networks of Salt Typhoon", *CyberScoop,* (May 21, 2025); https://cyberscoop.com/salt-typhoon-chinese-hackers-us-telecom-breach/.

[4] Memorandum, "Salt Typhoon: Data Theft Likely Signals Expanded Targeting", *Department of Homeland Security, Office of Intelligence and Analysis*, (Jun. 11, 2025); https://www.documentcloud.org/documents/25998809-20250611-dhs-salt-typhoon/.

[5] Nickel, Dana, "Salt (Typhoon) in the Wound", *Politico,* (Jul. 18, 2025); https://subscriber.politicopro.com/newsletter/2025/07/salt-typhoon-in-the-wound-00461756.

[6] "Weathering the storm: In the midst of a Typhoon", *Cisco Talos,* (Feb. 20, 2025); https://blog.talosintelligence.com/salt-typhoon-analysis/.

[7] 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.

I appreciate that Mandiant is a widely respected digital forensics and incident response provider with an extensive history cooperating with congressional oversight requests in the aftermath of major cybersecurity incidents.[8] Accordingly, please provide the following documents no later than August 6, 2025:

1. A copy of all reports, assessments, and analyses Mandiant conducted for AT&T and Verizon, respectively, in response to the Salt Typhoon attacks.
2. A list of any recommendations by Mandiant that have not been fully addressed by AT&T or Verizon in response to the Salt Typhoon attacks.
3. All records related to the costs and expenses of Mandiant's work for AT&T and Verizon, respectively, in response to the Salt Typhoon attacks.

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

[8] *See e.g.,* Report, "The Equifax Data Breach" Majority Staff Report, *U.S. House Committee on Oversight and Government Reform,* (Dec. 2018); https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.