United States Senate
WASHINGTON, DC 20510

November 14, 2024

VIA ELECTRONIC TRANSMISSION

John Stankey
Chief Executive Officer
AT&T Inc.

Dear Mr. Stankey:

I am concerned about recent reporting stating that the China-backed hacking group, Salt Typhoon, gained access to Call Detail Records, which contains information on who, when and how often Americans talk to, as well as location data.[1] According to these reports, Verizon, Lumen, and AT&T were among several companies that were breached, which resulted in the collection of data from an unknown number American citizens, including current and former government officials.[2] Additionally, the Wall Street Journal reported that, "[i]n Salt Typhoon, the actors linked to China burrowed into America's broadband networks. In this type of intrusion, bad actors aim to establish a foothold within the infrastructure of cable and broadband providers that would allow them to access data stored by telecommunications companies or launch a damaging cyberattack."[3] Unfortunately, as of November 6, 2024, according to reporting, the public does not know the breadth and severity of this attack.[4] AT&T must explain how this cyberattack happened and what is being done to ensure the security of data, as well the critical infrastructure it stewards.

I've previously raised concerns about the need to protect our nation's cybersecurity and U.S. critical infrastructure from national security threats.[5] On November 1, 2024, I wrote to the Department

[1] Sarah Krouse, Robert McMillan, and Dustin Volz, *China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack*, WALL STREET JOURNAL (Sep. 26, 2024), https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835?mod=article; *see also* John Sakellariadis, *Chinese hackers gained access to huge trove of Americans' cell records*, POLITICO (Nov. 6, 2024), https://www.politico.com/news/2024/11/06/chinese-hackers-american-cell-phones-00187873.
[2] *Id; see* Robert Legare, et al, *Trump, Vance, Harris campaign potential targets in broad China-backed hacking operation*, CBS NEWS (Oct. 25, 2024), https://www.cbsnews.com/news/trump-vance-potential-targets-china-backed-hacking-operation/.
[3] Krouse, *supra* note 1.
[4] Sakellariadis, *supra* note 1. ("The Biden administration first acknowledged it was investigating 'unauthorized access to commercial telecommunications infrastructure" by Chinese hackers two weeks ago. But it has been tightlipped about the cyber intrusion since, even as press reports have emerged suggesting it is one of the most serious breaches in recent years.'").
[5] Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Alejandro Mayorkas, Secretary, Department of Homeland Security, the Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency, and Mr. Ronald R. Rowe, Acting Director, United States Secret Service (Nov. 1, 2024), https://www.grassley.senate.gov/imo/media/doc/grassley_to_cisa_-_cyberattack.pdf; Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Merrick Garland, Attorney General, Department of Justice, and the Honorable Christopher Wray, Director, Federal Bureau of Investigation (Nov. 1, 2024), https://www.grassley.senate.gov/imo/media/doc/grassley_to_doj_and_fbi_-_salt_typhoon_cyberattack.pdf; Press Release, Sen. Charles E. Grassley, *Grassley Conducts Sweeping Oversight of Recent AT&T Hack, Potential National Security Implications* (Aug. 5, 2024), https://www.grassley.senate.gov/news/news-releases/grassley-conducts-sweeping-oversight-of-recent-atandt-hack-potential-national-security-implications; Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (July 3, 2024), https://www.grassley.senate.gov/imo/media/doc/grassley_to_cisa_-_cyberattack.pdf; *see also* Press Release, Sen. Charles E. Grassley, *Grassley: Federal Agencies Must Stop 'Dragging Their Feet' On Bolstering Cybersecurity Defense* (Apr. 8, 2024), https://www.grassley.senate.gov/news/news-releases/grassley-federal-agencies-must-stop-dragging-their-feet-on-bolstering-cybersecurity-defense.

of Homeland Security and its component agencies, as well the Department of Justice and the Federal Bureau of Investigation requesting information about the Salt Typhoon cyberattack, as well as the steps the agencies are taking to protect American citizens and government officials from these types of attacks.[6]

In August, I wrote to 17 federal agencies and AT&T regarding a cyberattack on the telecommunications company, which resulted in exposure to over 90 million Americans' data, potentially including federal agencies' communications patterns.[7] I also wrote to CISA on July 3, 2024, regarding a recent cyberattack, which released "critical information about the operation of U.S. infrastructure."[8] Additionally, on April 8, 2024, I wrote letters to seven of the Sector Risk Management Agencies responsible for overseeing our nation's critical infrastructure to highlight the threat of cyberattacks on our critical infrastructure sectors.[9] It is imperative that our federal agencies and private companies work together to ensure all data and critical infrastructure is safe and secure against future attacks.

In response to my August 2, 2024, letter, AT&T failed to provide full and complete answers to the questions I raised, as well as the documents I requested.[10] Additionally, my staff spoke with AT&T representatives on October 10, 2024, after receiving several responses from various federal agencies confirming that AT&T devices used by the federal government had been affected by the April 14-25, 2024, cyberattack.[11] The lack of transparency by AT&T is alarming, and I request full and complete responses, including the requested records, to my April 2, 2024, letter, as well as the additional questions that have been raised by the responses from federal agencies, which my staff emailed to you on October 10, 2024.[12] Specifically, my staff noted that in a letter from the Department of Defense (DOD), which confirmed DOD devices had been subject to the April 2024 attack, "AT&T informed the Department that they conducted forensic reviews and an investigation and continue to work closely with federal law enforcement and a team of external cybersecurity experts." My staff requested AT&T provide all internal and external forensic reviews and investigative materials.[13] Additionally, my staff asked AT&T whether the FBI has directed the company to not comply with Congressional oversight requests related to the April 2024 data breach and the Salt Typhoon hack.[14]

Accordingly, so Congress may conduct objective and independent oversight concerning the Salt Typhoon cyberattack, please provide answers to the following no later than November 28, 2024:

1. How and when did AT&T discover the cyberattack? Provide all records from AT&T internal investigation into this incident. [15]

---

[6] Nov. 1, 2024, to Mayorkas et. al., *supra* note 5; Nov. 1, 2024, to Garland et. al., *supra* note 5.
[7] *Grassley Conducts Sweeping Oversight of Recent AT&T Hack, Potential National Security Implications*, *supra* note 5.
[8] July 3, 2024, to Easterly *supra* note 5.
[9] *Grassley: Federal Agencies Must Stop 'Dragging Their Feet' On Bolstering Cybersecurity Defense*, *supra* note 5.
[10] On File with Committee Staff.
[11] Responses and Notes on File with Committee Staff.
[12] Emails on File with Committee Staff.
[13] *Id*.
[14] *Id*.
[15] "Records" include any written, recorded, or graphic material of any kind, including letters, memoranda, reports, notes, electronic data (emails, email attachments, and any other electronically created or stored information), calendar entries, inter-office communications, meeting minutes, phone/voice mail or recordings/records of verbal communications, and drafts (whether they resulted in final documents).

2. When did AT&T alert federal authorities regarding the data breach? Provide all records.

3. How many federal agencies, departments, or organizations were impacted or potentially impacted by the Salt Typhoon cyberattack? Has AT&T communicated with all of these entities? If not, why not?

4. Was AT&T aware of any potential vulnerabilities before the Salt Typhoon cyberattack? If so, what measures did AT&T take to secure customers' data? Provide all records.

5. What specific steps is AT&T taking to secure its data from future data breaches and cyberattacks? Provide all records.

6. Did any federal agency warn AT&T of a potential cyberattack by Salt Typhoon or other entity? If so, what agencies and when? Provide a list of all warnings and actors.

7. Provide copies of internal and external cybersecurity audits in the last five years.

8. Provide copies of all contracts that AT&T currently has with the Executive, Judicial, and Legislative branches.

9. Does AT&T employ any legacy IT systems? Were those accessed during the Salt Typhoon cyberattack?

Thank you for your prompt review and responses. If you have any questions, please contact Tucker Akin on my Committee staff at (202) 224-0642.

Sincerely,

Charles E. Grassley
Ranking Member
Committee on the Budget