United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510–6275

January 15, 2025

VIA ELECTRONIC TRANSMISSION

Paul Sunu
Chairman and CEO
Windstream

Dear Mr. Sunu:

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 Americans talk to, when and how often, as well as location data.[1] According to these reports, Verizon, Lumen, AT&T, T-Mobile, Charter Communications, Consolidated Communications, and Windstream were among several companies that were breached, which resulted in the collection of data from an unknown number of American citizens, including current and former government officials.[2] Reporting also notes that Salt Typhoon hackers "unpatched network devices" from Fortinet and "compromised large network routers" from Cisco Systems, as well as routers built by Netgear.[3] 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."[4] Unfortunately, according to reporting, the public does not know the breadth and severity of this attack, despite it being called the "worst telecom hack in our nation's history."[5] Windstream must explain how this cyberattack happened and what is being done to ensure the security of the data, as well the critical infrastructure, it stewards.

---

[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/; *see also* Sarah Krouse, Dustin Volz, *T-Mobile Hacked in Massive Chinese Breach of Telecom Networks*, WALL STREET JOURNAL (Nov. 14, 2024), https://www.wsj.com/politics/national-security/t-mobile-hacked-in-massive-chinese-breach-of-telecom-networks-4b2d7f92?msockid=2c7a053cbcee6f980b4a111fbdfc6ea2.

[3] Dustin Volz, Aruna Viswanatha, Sarah Krouse, and Drew Fitzgerald, *How Chinese Hackers Graduated From Clumsy Corporate Thieves to Military Weapons*, WALL STREET JOURNAL (Jan. 4, 2025), https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95?msockid=2c7a053cbcee6f980b4a111fbdfc6ea2.

[4] Krouse, *supra* note 1.

[5] 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.'"); *see also* Ellen Nakashima, *Top senator calls Salt Typhoon 'worst telecom hack in our nation's history'*, WALL STREET JOURNAL (Nov. 21, 2024), https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/. ("The hackers, part of a group dubbed Salt Typhoon, have been able to listen in on audio calls in real time and have in some cases moved from one telecom network to another, exploiting relationships of "trust," said Sen. Mark R. Warner (D-Virginia), chairman of the Senate Intelligence Committee and a former telecom venture capitalist. Warner added that intruders are still in the networks.").

On November 14, 2024, I wrote letters to Lumen, Verizon, and AT&T regarding Salt Typhoon.[6] Further, on November 26, 2024, I wrote a letter to T-Mobile regarding Salt Typhoon.[7] Additionally, I previously raised concerns about the need to protect our nation's cybersecurity and U.S. critical infrastructure from national security threats.[8] On November 1, 2024, I wrote to the Department of Homeland Security and its component agencies, as well the Department of Justice and the Federal Bureau of Investigation (FBI) 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.[9]

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.[10] I also wrote to CISA on July 3, 2024, regarding a recent cyberattack, which released "critical information about the operation of U.S. infrastructure."[11] 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.[12] 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.

Accordingly, so Congress may conduct objective and independent oversight concerning the Salt Typhoon cyberattack, please provide answers to the following no later than January 29, 2025:

1. How and when did Windstream discover the cyberattack? Provide all records from Windstream's internal investigation into this incident. [13]

---

[6] Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to Kate Johnson, CEO, Lumen Technologies, Hanz Vestberg, Chairman and CEO, Verizon Communications Inc., and John Stankey, CEO, AT&T Inc. (Nov. 14, 2024), https://www.grassley.senate.gov/imo/media/doc/grassley_to_lumen_verizon_att_-_salt_typhoon.pdf.

[7] Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to Mike Sievert, Preisdent and CEO, T-Mobile US, Inc. (Nov. 26, 2024), https://www.grassley.senate.gov/imo/media/doc/grassley_to_t-mobile_-_salt_typhoon_cyberattack.pdf.

[8] 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.

[9] Nov. 1, 2024, to Mayorkas et. al., *supra* note 8; Nov. 1, 2024, to Garland et. al., *supra* note 8.

[10] *Grassley Conducts Sweeping Oversight of Recent AT&T Hack, Potential National Security Implications*, *supra* note 8.

[11] July 3, 2024, to Easterly *supra* note 8.

[12] *Grassley: Federal Agencies Must Stop 'Dragging Their Feet' On Bolstering Cybersecurity Defense*, *supra* note 8.

[13] "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. Did the Salt Typhoon hackers access any of Windstream's customer data? If so, what kinds of data were accessed? If so, has Windstream notified any of the affected customers? If not, why not? Provide all records.

3. When did Windstream alert federal authorities regarding the cyberattack? Provide all records.

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

5. Was Windstream aware of any potential vulnerabilities before the Salt Typhoon cyberattack? If so, what measures did Windstream take to secure customers' data, network infrastructure, and other systems Windstream operates? Provide all records.

6. What specific steps is Windstream taking to secure its data, network infrastructure, and other systems Windstream operates from future cyberattacks? Provide all records.

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

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

9. Provide copies of all contracts that Windstream currently has with the Executive, Judicial, and Legislative branches.

10. Does Windstream employ any legacy IT systems? Were those accessed during the Salt Typhoon cyberattack?

11. Does Windstream require multifactor authentication to access network management accounts? If not, why not? Was this requirement in place prior to the Salt Typhoon attack?

12. Does Windstream have any shared accounts or shared connections with any other telecommunications company affected by the Salt Typhoon attack? Did Salt Typhoon access any of these shared accounts or connections through Windstream?

Thank you for your prompt review and responses. If you have any questions, please contact Tucker Akin on my Committee staff at (202) 224-7708.

Sincerely,

Charles E. Grassley
Chairman
Committee on the Judiciary