Congress of the United States
House of Representatives
SELECT COMMITTEE ON THE CHINESE COMMUNIST PARTY

October 10, 2024

Mr. Hans Vestberg
Chairman and Chief Executive Officer
Verizon
1095 Avenue of the Americas
New York, NY 10036

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

Ms. Kate Johnson
President and Chief Executive Officer
Lumen Technologies
100 CenturyLink Drive
Monroe, LA 71203

Dear Mr. Vestberg, Mr. Stankey, and Ms. Johnson:

On October 5, the *Wall Street Journal* reported that "a cyberattack tied to the Chinese government penetrated the networks of a swath of U.S. broadband providers, potentially accessing information from systems the federal government uses for court-authorized network wiretapping requests. For months or longer, the hackers might have held access to network infrastructure used to cooperate with lawful U.S. requests for communications data"[1] This article specifically cites your three companies as victims of this potential CCP-sponsored hack.

The implications of any breach of this nature would be difficult to overstate. According to one senior U.S. intelligence official quoted in the *Washington Post,* "it enables [the CCP] to understand exactly who the U.S. government is interested in and to either undermine the government's intelligence collection efforts or to feed the United States disinformation."[2]

[1] https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b
[2] https://www.washingtonpost.com/national-security/2024/10/06/salt-typhoon-china-espionage-telecom/

Accordingly, it comes as no surprise that the group publicly reported to likely be behind this attack is Salt Typhoon, a hacking unit closely affiliated with the PRC's Ministry of State Security.

Earlier this year, the Select Committee held a hearing focused on another PRC hacking group, known as Volt Typhoon, and its successful efforts to compromise U.S. critical infrastructure. Taken together with these news reports regarding Salt Typhoon's apparent compromise of our nation's wiretap system, it is clear that we face a cyber-adversary the likes of which we have never confronted before, and we must urgently enhance our nation's approach to cybersecurity.

We recognize that enhancing our nation's cybersecurity is a challenge that neither the public nor private sectors can tackle alone. While we appreciate that there may be an ongoing federal investigation into this matter, and we appreciate your cooperation with any such inquiries, we cannot wait to fortify our defenses. Accordingly, we respectfully request a closed-door briefing from appropriate representatives of each of your companies regarding the reported Salt Typhoon breach. At this briefing, please address the following matters.

- Please describe when your companies first became aware of matters described in the *Wall Street Journal* article.
- Please describe any specific measures your companies are taking to protect systems the federal government uses for court-authorized network wiretapping requests.
- Please describe what measures Congress and the federal government can undertake to help your companies implement additional measures to protect against PRC state-sponsored hacking efforts.

Thank you for your attention to this matter. We stand ready to support your companies and other critical infrastructure operators in protecting against PRC-based cyber threats.

Sincerely,

John Moolenaar
Chairman

Raja Krishnamoorthi
Ranking Member