

Congress of the United States
Washington, DC 20515

June 5, 2025

The Honorable Secretary Kristi Noem
Secretary
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Avenue SE
Washington, DC 20528

The Honorable Tulsi Gabbard
Director
Office of the Director of National Intelligence
1500 Tysons McLean Drive
McLean, VA 22102

Dear Secretary Noem and Director Gabbard:

We are writing to sound the alarm about perhaps the single greatest latent threat to the national and homeland security of the United States: the cyber threat posed by the Chinese Communist Party.

Salt Typhoon and Volt Typhoon, cyber campaigns sponsored by the Chinese Communist Party (CCP), mark a new and insidious inflection point in the history of ever-escalating cyber conflict. With the Volt Typhoon campaign, an adversarial foreign power has all but infiltrated our networks for the purpose of not only espionage but also sabotage, prepositioning itself to activate malware that would decimate American critical infrastructure in the event of a crisis. Volt Typhoon is a loaded gun aimed squarely at America, ready to be triggered as a weapon of war.

This is not a one-time invasion. Salt Typhoon represents an unprecedented occupation of American telecom networks. It has been described as the “worst telecom hack in our nation's history[,]”¹ providing the CCP with unparalleled opportunities for espionage, and as the FBI has stated, in fact “resulted in the theft of call data logs, a limited number of private communications involving identified victims, and the copying of select information subject to court-ordered US law enforcement requests.”²

The cyber threat is not only confined to the nation’s telecom systems—it likely runs the gamut of energy, finance, healthcare, transportation, and water. The CCP’s cyber gangs are not collecting valuable intelligence but are pre-positioning for strategic and systemic disruption, lying in wait for a precipitating event like a conflict in the Taiwan Strait. In fact, as demonstrated by the separate Volt Typhoon attacks, “People’s Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.”³

All of which raises a sobering question: Who in the Trump Administration is in charge of eradicating the CCP from our most critical infrastructure? The answer is dangerously unclear.

Instead of rising to meet the moment, the Trump Administration appears intent on dismantling the core institutions responsible for cyber defense. The Cyber Safety Review Board, designed to investigate incidents like Salt Typhoon, has been all but abolished. The Cybersecurity and Infrastructure Security Agency (CISA)—our nation’s lead civilian authority for cyber coordination and infrastructure protection—is being hollowed-out. The Trump Administration is proposing to cut CISA’s budget by a half a billion dollars and reduce its staff by up to 1300. Somewhere, Xi Jinping is smiling at America’s insistence on degrading its own cyber capabilities.

¹ Wendling, Mike. “What to Know about String of US Hacks Blamed on China.” *BBC News*, BBC, 31 Dec. 2024, www.bbc.com/news/articles/c86w2evj05do.

² “FBI Seeking Tips about PRC-Targeting of US Telecommunications.” *Internet Crime Complaint Center (IC3) | FBI Seeking Tips about PRC-Targeting of US Telecommunications*, www.ic3.gov/PSA/2025/PSA250424-2.

³ “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure: CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, 21 May 2025, www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

Given America's declining cyber defenses in an age of rising cyber threats, I respectfully request that you provide clear answers to the following questions:

1. Who has been designated within the Trump Administration to lead the response to the Salt Typhoon breach? Who has been designated to lead the investigation, and what is the status of any ongoing investigatory efforts?
2. Can you publicly confirm whether or not U.S. telecom networks continue to be compromised? Please provide a timeline of any related efforts to address the Salt Typhoon breach.
3. Can you publicly confirm whether or not U.S. critical infrastructure networks continue to be compromised by the Volt Typhoon breach? Who has been designated within the Trump Administration to lead the response to threats Volt Typhoon?
4. What interagency structures, if any, remain intact to oversee, coordinate, and implement a cyber response to Volt Typhoon and the investigation of Salt Typhoon?
5. What is the status of eradication efforts that have been undertaken for both Salt Typhoon and Volt Typhoon?
6. What is the impact of CISA's budget cuts and staffing reductions on the federal government's ability to address Salt Typhoon and Volt Typhoon?

This is not a partisan issue. It is a matter of grave consequence for the security of America both at home and abroad. We owe it to the American people to protect them from the specter of a cyber 9/11 at the hands of our most formidable foreign adversary.

We implore you to treat the matter with the urgency it clearly deserves. We look forward to your detailed response.

Sincerely,



Ritchie Torres
Member of Congress



Raja Krishnamoorthi
Member of Congress



Kathy Castor
Member of Congress



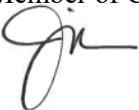
Ro Khanna
Member of Congress



Haley Stevens
Member of Congress



Shontel Brown
Member of Congress



Jill Tokuda
Member of Congress