United States Senate

WASHINGTON, DC 20510

November 12, 2025

The Honorable Kristi Noem
Secretary
Department of Homeland Security
Washington, D.C. 20016

The Honorable Tulsi Gabbard
Director of National Intelligence
Office of the Director of National Intelligence
Washington, D.C. 20511

Dear Secretary Noem and Director Gabbard:

We write to request that you release to the public an unclassified report titled "U.S. Telecommunications Insecurity 2022," which is critically important to U.S. national security, but which the Department of Homeland Security (DHS) has inexplicably failed to release for the past nine months. Given the continuing threat of adversary compromise of insecure U.S. telecommunications infrastructure, we also request that you encourage the Federal Communications Commission (FCC) to maintain mandatory minimum cybersecurity standards for our communications sector.

As you know, in November 2024, the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency (CISA) publicly confirmed a major hack of U.S. telecommunications carriers by actors affiliated with the Chinese government. Through these compromises, the Chinese government reportedly targeted the communications of senior U.S. officials and maintained deep access to sensitive communications infrastructure. The Salt Typhoon compromise represents one of the most serious espionage campaigns against the communications of U.S. government leaders in history, and highlighted important gaps in our nation's communications security — in some cases, with providers ignoring basic security precautions such as credential re-use across network appliances and failure to adopt multi-factor authentication for highly privileged network administrator accounts.

The Salt Typhoon hack is not the only counterintelligence and national security threat to the U.S. communications sector. Foreign adversaries — including non-state actors — have been able to exploit longstanding vulnerabilities in U.S. phone networks to track phones, tap calls and texts, and remotely infect phones with spyware. DHS documented these issues in a public report to Congress over eight years ago. A recent compromise by nation-state actors of a major service-provider to U.S. communications firms suggests that significant threats to this sector continue.

Collectively, these compromises highlight the urgency of securing U.S. communications networks from foreign threats. Perplexingly, rather than conducting a comprehensive inquiry, the Administration fired the Cyber Safety Review Board, which had been directed to engage in such an effort. Moreover, FCC Chair Brendan Carr recently announced his plans to reverse a prior FCC effort to drive more effective security practices in the telecommunication sector.

The continued suppression of a report identifying serious vulnerabilities of the U.S. telecommunications sector undermines the public's understanding of these threats and stymies an important public debate on a path forward to secure the U.S. telecommunications sector and protect the U.S. Government and all Americans who rely on that sector. This July, the Senate unanimously passed the Telecom Cybersecurity Transparency Act, a bill requiring the Secretary of Homeland Security to publish this report in full. Shortly thereafter, CISA released a statement to the press stating that the agency intended to release the report; however, three months later, the report remains hidden from the American public.

During Director Gabbard's confirmation process, she noted that the hack "highlight[ed] the vulnerabilities in our critical infrastructure that must be urgently addressed, as well as China's sophisticated cyber capabilities and efforts to gather sensitive government data" and told the Senate Intelligence Committee that she would use her position to "advocate for policies, practices or legislation to strengthen cyber protections in the telecommunications sector."

We urge you to ensure the immediate public release of the unclassified CISA report, "U.S. Telecommunications Insecurity 2022," and to call for the FCC to establish mandatory minimum cybersecurity standards for the communications sector due to the risk of vulnerabilities presenting a significant threat to U.S. Government communications and security and the country.

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden
United States Senator

Mark R. Warner
United States Senator