MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Eighteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

October 18, 2024

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
1110 N. Glebe Road
Arlington, VA 20598-0630

The Honorable Christopher A. Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Dear Director Easterly and Director Wray:

As you well know, the threats posed by People's Republic of China (PRC)-backed cyber actors to U.S. networks and critical infrastructure are intensifying. Given recent reporting on Salt Typhoon, which has specifically targeted major internet service providers (ISPs) such as AT&T, Verizon, and Lumen Technologies, we write with heightened urgency about the Cybersecurity and Infrastructure Security Agency's (CISA) and the Federal Bureau of Investigation's (FBI) roles in mitigating and defending against PRC-backed threats.[1] If reporting about Salt Typhoon's level of network access is accurate, the PRC could influence communications by rerouting internet traffic, [2] or gain valuable information by accessing systems for lawful wiretapping requests.[3] In other words, this intrusion would significantly jeopardize Americans' right to privacy and broader U.S. national security interests.

We appreciate the continued efforts by U.S government agencies, including CISA and the FBI, to raise awareness about the pre-positioning activities of Volt Typhoon and other PRC-backed cyber threat actors. However, we are extremely concerned about what Salt Typhoon's intrusion may imply about the state of America's cyber resiliency. As America's cyber defense agency, we expect CISA to continue playing a pivotal role in educating Americans about cyber risks. Additionally, we urge CISA to conduct more direct outreach to our critical infrastructure

[1] Sarah Krouse et al., "*U.S. Wiretap Systems Targeted in China-Linked Hack*," WSJ, (Oct. 5, 2024), https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b
[2] Sarah Krouse et al., "*China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack*," WSJ, (Sept. 26, 2024), https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835?mod=article_inline
[3] *Id* at 1.

owners and operators to ensure they are prepared to identify and thwart malicious activity in their networks and infrastructure.

The Committee has taken the threat of PRC-backed cyber actors, including Volt Typhoon, seriously. Last month, we unanimously passed H.R. 9769, the *Strengthening Cyber Resilience Against State-Sponsored Threats Act*, which directs CISA and the FBI to create a task force that better prioritizes and coordinates U.S. government efforts to defend against PRC-backed cyber threat actors. Although we are encouraged to hear that CISA is participating in a new "emergency team" to address the Salt Typhoon hack, clearly a temporary measure will not suffice.[4] Reporting indicates that Salt Typhoon has been active since 2020,[5] and PRC-backed threats against Western nations primarily aimed at intelligence collection show no sign of waning.[6]

On August 6, 2024, CISA and the FBI provided the Committee's staff with a briefing on the state of PRC cyber threats, and we are grateful for the information shared at that time.[7] However, given escalating concerns about Salt Typhoon, we believe it is necessary for the Committee to receive an updated assessment of trends and U.S. efforts to defend against PRC-affiliated cyber actors. Accordingly, we request a briefing from CISA and the FBI by no later than 5:00 p.m. on November 1, 2024.

Per Rule X of the U.S House of Representatives, the Committee on Homeland Security is the principal committee of jurisdiction for overall homeland security policy, and has special oversight functions of "all Government activities relating to homeland security, including the interaction of all departments and agencies with the Department of Homeland Security."

Please contact the Committee on Homeland Security Majority Staff at (202) 226-8417 with any questions about this request. We appreciate your attention to this issue and anticipate your prompt reply.

Sincerely,

MARK E. GREEN, M.D.
Chairman
Committee on Homeland Security

ANDREW R. GARBARINO
Chairman
Subcommittee on Cybersecurity and Infrastructure Protection

---

[4] Ellen Nakashima, "*White House forms emergency team to deal with China espionage hack*," The Wash. Post, (Oct. 11, 2024), https://www.washingtonpost.com/national-security/2024/10/11/china-hack-telecoms-salt-typhoon/
[5] Megan Morrone, "*What you need to know about the Salt Typhoon hack*," Axios, (last accessed Oct. 15, 2024), https://www.axios.com/2024/10/15/salt-typhoon-hack-china-verizon-att
[6] Max Colchester and Daniel Michaels, "*Scale of Chinese Spying Overwhelms Western Governments*," WSJ, (Oct. 14, 2024), https://www.wsj.com/politics/national-security/scale-of-chinese-spying-overwhelms-western-governments-6ae644d2
[7] H. Comm. on H. Sec. briefing with Fed. Bureau of Inv. and Cybersecurity and Inf. Sec. Agency (August 6, 2024).

LAUREL LEE
Member
Committee on Homeland Security

Encl.

cc: The Honorable Bennie Thompson, Ranking Member
Committee on Homeland Security