



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

March 17, 2025

The Honorable Kristi Noem
Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Noem:

The Committee on Homeland Security (Committee) is conducting oversight of the federal response to the malicious cyber campaigns against U.S. critical infrastructure conducted by Volt and Salt Typhoon, two advanced persistent threat actors that are sponsored by the People's Republic of China (PRC).

Last year, Volt and Salt Typhoon grabbed headlines for successfully compromising U.S. critical infrastructure with sophisticated tactics. For example, in February 2024, U.S. government agencies revealed that Volt Typhoon had burrowed for at least five years into the information technology environments of several key critical infrastructure sectors, including energy, water and wastewater systems, transportation systems, and communications.¹ In September 2024, the Wall Street Journal reported that another PRC state-sponsored threat actor, Salt Typhoon, had breached leading U.S. internet-service providers,² targeting individuals such as then-former President Donald Trump and then-vice presidential nominee J.D. Vance.³

Despite officials raising the alarm about Volt and Salt Typhoon, we still know very little about them – except that Volt Typhoon, in particular, continues to compromise our critical infrastructure. In January 2024, then-Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly testified that CISA is “working aggressively with our partners in industry and across the U.S. Government to take action now, knowing that this threat [Volt Typhoon] is real and this threat is urgent.”⁴ However, we remain gravely concerned that the Biden

¹ Cybersecurity Advisory, Cybersecurity and Infrastructure Security Agency, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (Feb. 7, 2024), available at <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

² Sarah Krouse et al., *China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack*, WALL ST. J., Sept. 26, 2024, <https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835>.

³ Sam Sabin *What to Know About Salt Typhoon's Latest Attack*, AXIOS, Oct. 29, 2024, <https://www.axios.com/2024/10/29/salt-typhoon-targets-politicians-phones>.

⁴ *The CCP Cyber Threat to the American Homeland and National Security: A Hearing Before the H. Select Comm. on the Strategic Competition Between the United States and the Chinese Communist Party*, 118th Cong., 24 (2024)

Administration failed to mitigate these significant threats posed by the PRC. In fact, the Biden Administration delayed providing a briefing on Salt Typhoon to the Committee until about a month after the Wall Street Journal broke the news about the threat actor's activity.

On January 15, 2025, then-CISA Director Jen Easterly stated in a release that CISA, industry, and other federal partners "have been laser focused on deterring China's cyber aggression," specifically referencing Volt and Salt Typhoon.⁵ These threat actors pose significant challenges that cannot be addressed overnight. The Biden Administration's lack of transparency surrounding the federal government's response to Volt and Salt Typhoon, however, was unacceptable and disconcerting.

As National Coordinator of Critical Infrastructure Security and Resiliency, CISA plays a pivotal role in the nation's response to Volt and Salt Typhoon. CISA must be prepared and equipped to rapidly respond in times of crisis, as well as accountable to its stakeholders across the public and private sectors. The Committee seeks to examine CISA's response to Volt and Salt Typhoon to ensure CISA is focused on, and empowered to perform, its core mission effectively. Additionally, given the cross-sector impact of these PRC-backed threat actors, the Committee seeks to understand the role of other U.S. government entities is necessary for ensuring the resilience of America's cybersecurity posture.

The extent of Volt Typhoon's activities became public more than a year ago. It is the Committee's hope that the Trump Administration will provide the American people with confidence that their government is taking every step possible to mitigate the impact of Volt and Salt Typhoon on government entities and businesses. If the Biden Administration was negligent in its response, we must hold accountable those responsible for failing to mitigate one of the greatest modern-day threats to the homeland.

To assist the Committee with its oversight of the federal government's response to the Volt and Salt Typhoon intrusions, please provide the following documents and information as soon as possible, but no later than 5:00 p.m. on March 31, 2025:

1. All documents and communications, including but not limited to, e-mail, internal memoranda, and guidance, referring or relating to Volt Typhoon and Salt Typhoon from January 20, 2021, to the present date.
2. Documents sufficient to explain when DHS and CISA became aware of the cybersecurity threats, cyber intrusion attempts, and damages caused by Volt Typhoon and Salt Typhoon; and

(statement of Jen Easterly, Dir., Cybersecurity and Infrastructure Security Agency), *available at* <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/1.31.24%20Hearing%20Transcript.pdf>.

⁵ Posting of Jen Easterly to Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats> (Jan. 15, 2025).

3. Documents sufficient to identify a timeline of events related to CISA's responses to Volt Typhoon and Salt Typhoon, including actions taken with relevant Agencies/Departments, industry stakeholders, victims, and any other relevant parties once the threat from Volt Typhoon and Salt Typhoon was detected.

An attachment contains instructions for responding to this request. Please contact the Committee on Homeland Security Majority staff at (202) 226-8417 with any questions about this request.

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 of "all Government activities relating to homeland security, including the interaction of all departments and agencies with the Department of Homeland Security."

Thank you for your prompt attention to this important matter.

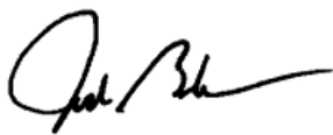
Sincerely,



MARK E. GREEN, M.D.
Chairman



ANDREW R. GARBARINO
Chairman
Subcommittee on Cybersecurity and
Infrastructure Protection



JOSH BRECHEEN
Chairman
Subcommittee on Oversight, Investigations,
and Accountability

Encl.

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

Secretary Noem
March 17, 2025
Page 4

The Honorable Eric Swalwell, Ranking Member
Subcommittee on Cybersecurity and Infrastructure Protection

The Honorable Shri Thanedar, Ranking Member
Subcommittee on Oversight, Investigations, and Accountability