JD VANCE
OHIO

United States Senate
WASHINGTON, DC 20510

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
SPECIAL COMMITTEE ON AGING
JOINT ECONOMIC COMMITTEE

May 10, 2024

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
1100 Hampton Park Blvd.
Capitol Heights, MD 20743-0630

Director Easterly:

I write to express my concern that U.S. critical infrastructure appears to be under attack from the PRC state-sponsored hacker group known as Volt Typhoon. The impact from a full-scale Volt Typhoon attack on U.S. critical infrastructure would be devastating and could result in our nation being thrown into disarray at the exact time it is under military attack from foreign adversaries. The consequences of a Volt Typhoon attack would presumably include a threat to the U.S. military by disrupting power and water to our military facilities and critical supply chains.

According to reports, Volt Typhoon has compromised hundreds of thousands of devices since it was publicly identified by Microsoft in May 2023.[1] Indeed, experts believe the group has targeted U.S. critical infrastructure since mid-2021 using malicious software that penetrates internet-connected systems. On January 31, 2024, the FBI reported that it had disrupted some of Volt Typhoon's operations by removing the group's malware from some small office routers.[2] However, on February 7, 2024, CISA, the FBI, and other U.S. agencies along with the Five Eyes partners released a major advisory in which they warned that Volt Typhoon was pre-positioning on critical infrastructure networks to "enable disruption or destruction of critical services in the event of increased geopolitical tensions."[3] According to the agencies, "this is a critical business risk for every organization in the United States and allied countries."[4] On March 19, 2024, CISA along with other agencies released a fact sheet advising critical infrastructure executive leaders

[1] *Volt Typhoon Targets U.S. Critical Infrastructure with Living-off-the-Land Techniques,* Microsoft Threat Intelligence, May 24, 2023.
[2] *U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure*, DOJ Office of Public Affairs, January 31, 2024.
[3] *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, CISA, February 7, 2024.
[4] *Id.*

"on the urgent risk posed"[5] by Volt Typhoon and how to mitigate the threat of attack to the Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors.

Following Secretary of State Blinken's April visit to China, Ambassador Fick stated that Secretary Blinken was "very clear that holding American critical infrastructure at risk — especially civilian critical infrastructure — is dangerous. It's escalatory. It's unacceptable."[6] Ambassador Fick added that the U.S. delegation spoke with the Chinese officials "about Volt Typhoon directly."[7] According to press reports, President Joe Biden also addressed Volt Typhoon in meetings with Chinese President Xi Jinping.

To better understand this risk, please provide answers to the following questions by COB on May 24, 2024:

1. What is CISA's understanding of how Volt Typhoon became embedded in U.S. critical infrastructure?
2. What prompted CISA to go public earlier this year warning of the urgent risk posed by Volt Typhoon?
3. How many U.S. public or private critical infrastructure entities in the Communications, Energy, Transportation Systems, and Water and Wastewater Systems sectors are impacted by Volt Typhoon?
4. Are there other critical infrastructure sectors impacted by Volt Typhoon? If so, which sectors (beyond those named in response to question 3)?
5. According to reports, CISA has worked with sector risk management agencies to do outreach to each sector regarding Volt Typhoon. Which agencies specifically?
6. Which Information Sharing and Analysis Centers (ISACs) are aware of Volt Typhoon?
7. How many individual network devices in the U.S. are impacted or potentially impacted by Volt Typhoon?
8. What strategies have CISA and/or sector risk management agencies named in response to question 5 designed and/or implemented to mitigate the threat from Volt Typhoon?
9. How many calls to CISA's 24/7 Operations Center regarding Volt Typhoon has the agency received since January 1, 2023?

Sincerely,

JD Vance
United States Senator

[5] *PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders*, CISA, March 19, 2024.
[6] *Volt Typhoon operation came up 'directly' in US-China talks, ambassador says*, The Record, May 7, 2024.
[7] *Id.*