Congress of the United States
Washington, DC 20515

August 3, 2023

Hon. Lloyd J. Austin III
Secretary of Defense
Department of Defense
1500 Pennsylvania Avenue NW
Washington, DC 20220

Mr. Rob Joyce
Director of Cyber Security
National Security Agency
9800 Savage Rd., Suite 6272
Fort George G. Meade, MD 20755

Dear Secretary Austin and Director Joyce:

Recent reports of Chinese malware embedded in the software operating power grids, communications systems, and water distribution systems supporting U.S. military installations are cause for great concern.[1] These Communist Chinese Party (CCP) malware reports appear to be part of an increasingly aggressive CCP espionage campaign. While not inclusive of all CCP efforts, they include unclassified examples such as the spy balloon that crossed sovereign U.S. territory, targeted hacking[2] of U.S. Ambassador to Beijing Nicholas Burns and Commerce Secretary Gina Raimondo's government emails, and malware attacks[3] on communications systems in Guam. Ensuring that we have the proper safeguards in place to protect our most critical infrastructure is of paramount importance in the face of increasing CCP aggression.

As the Administration attempts to confirm the source of this attack, we request that you keep members of the House Armed Services Committee—those tasked with direct oversight and policymaking for the Department of Defense and its cybersecurity efforts—informed of your findings and the plans to eliminate CCP operations in our networks and prevent future attacks. It is unacceptable that critical U.S. military installations and networks become compromised by any foreign actor. Our ability to defend the homeland and project power on a global scale must not be dissuaded.

The increase in CCP attacks on U.S. basing and military infrastructure are matched with their increasingly aggressive behaviors in the Taiwan Strait, Philippine Sea, and other international waters and airspace in the INDOPACOM region. Leaving CCP aggression unchecked only invites expanded CCP bellicose behaviors. CCP aggression in the Cyber Domain must be met with a firm, resolute, and measured response from the United States.

---

[1] **U.S. Hunts Chinese Malware That Could Disrupt American Military Operations**
https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html

[2] **Hacking of Government Email Was Traditional Espionage, Official Says**
https://www.nytimes.com/2023/07/20/us/politics/china-hacking-official-email.html

[3] **Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?**
https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html

Xi Jinping and the CCP have repeatedly made their threats against Taiwan clear and are becoming increasingly forward in surveilling and targeting the U.S. homeland as well. We cannot allow the CCP to cripple our resolve from the inside by infiltrating the critical infrastructure that enables U.S. force mobilization.

Due to the sensitivity of this matter and the urgency with which we must secure U.S. critical infrastructure, especially that which supports military operations and facilitates the Department of Homeland Security (DHS) in securing all U.S. Homeland critical infrastructure, we request your response to the following questions:

1. What is the extent of the Chinese cyber campaign(s) targeting U.S. military installations, and what specific critical U.S. infrastructure around U.S. military installations has been compromised?
2. How long has the Biden Administration been aware of the cyber campaign against the targeted systems, and what steps have been taken to restrict their access and prevent future attacks?
3. Given the access the Chinese hackers obtained, how damaging could the attack have been on U.S. military mobility and operations?
4. What guardrails are in place to protect our military critical infrastructure, including our electrical grid, communications systems, and water supply, particularly in responding to a contingency in the Indo-Pacific? What are the shortfalls and what is the Administration doing to close these gaps?

Please respond to these questions in writing by August 14, 2023, and provide members of the House Armed Services Committee with a full briefing on this situation upon Congress's return in September.

Sincerely,

Mark Alford
Member of Congress

Robert J. Wittman
Member of Congress

Michael Waltz
Member of Congress

Doug Lamborn
Member of Congress

Elise Stefanik
Member of Congress

Ronny L. Jackson
Member of Congress

Jen Kiggans
Member of Congress

Cory Mills
Member of Congress

Nancy Mace
Member of Congress

James Moylan
Member of Congress

Rich McCormick
Member of Congress

Joe Wilson
Member of Congress