Congress of the United States
Washington, DC 20515

May 10, 2023

The Honorable Alejandro Mayorkas
Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Mayorkas,

The Committee on Homeland Security and the Select Committee on the Strategic Competition between the United States and the Chinese Communist Party (Select Committee on China) (Committees) are conducting oversight of the presence of Chinese software and operational technology in U.S. port infrastructure. This includes software used for cranes, terminal industrial control systems, power systems, and telecommunications equipment.

On April 3, 2023, Members of the Committee on Homeland Security sent a letter to the Department of Homeland Security (DHS) requesting a briefing on DHS' maritime port security responsibilities.[1] The letter, among other requests, asked for documents sufficient to show DHS' efforts to address security vulnerabilities related to the use of Chinese-manufactured cranes at U.S. ports by April 17, 2023. To date, however, DHS has failed to provide a briefing or documentation, and these requests remain outstanding. We seek your immediate compliance.

We remain concerned about the security risks associated with the widespread use of Chinese-manufactured cranes that threaten to undermine our national security, particularly those made by Shanghai Zhenhua Heavy Industries (ZPMC), a Chinese state-owned business whose governing shareholder is China Communications Construction Company. We request additional information on the prevalence of such equipment and technology at U.S. ports and DHS actions to address the potential national security threats posed by the Chinese Communist Party's (CCP) use of this technology in U.S. port infrastructure.

ZPMC has operated under the umbrella of the Chinese state since its conception and has rapidly grown to be the dominant global manufacturer of ship-to-shore cranes.[2] Today, ZPMC controls around 70 percent of the global market share for cranes and accounts for nearly 80 percent of the ship-to-shore cranes in use at U.S. ports, posing significant risk to U.S. homeland security.[3] These security risks include cyberattacks, espionage, and supply chain vulnerabilities due to the shared software and interconnectivity among ZPMC cranes operating at our nation's ports. According to the *Wall Street Journal*, "[s]ome national-security and Pentagon officials have compared ship-to-shore cranes made by the China-based manufacturer, ZPMC, to a Trojan

---

[1] Letter from Rep. Mark E. Green, Chairman, H. Comm. on Homeland Sec. et al., to Hon. Alejandro Mayorkas, Sec'y, Dep't of Homeland Sec., (Apr. 3, 2023).
[2] Grady McGregor, *China's Crane Reign*, THE WIRE CHINA, Mar. 26, 2023, https://www.thewirechina.com/2023/03/26/chinas-crane-reign-zpmc.
[3] Aruna Viswanatha, Gordon Lubold, and Kate O'Keefe, *Pentagon Sees Giant Cargo Cranes as Possible Chinese Spying Tools*, WALL ST. J., Mar. 5, 2023, https://www.wsj.com/articles/pentagon-sees-giant-cargo-cranes-as-possible-chinese-spying-tools-887c4ade.

horse."[4] ZPMC cranes pose a potential risk for intelligence gathering purposes and we find it disconcerting that CCP-backed entities may use their access to ZPMC cranes to target and disrupt our nation's ports in the event of a Chinese invasion of Taiwan.

As stated recently in *Politico*, "President Joe Biden has committed multiple times to sending U.S. troops to Taiwan in the event of a Chinese invasion, something China would want to stop. This could include targeting the networks of ports on the West Coast, airfields, and other transportation networks that move troops."[5] These transportation networks include our nation's ports, pipelines, and freight railways. As a Co-Sector Risk Management Agency for the Transportation Systems Sector, DHS is responsible for securing these networks and providing response and recovery assistance to impacted entities.

In February 2023, Jen Easterly, the Director of the Cybersecurity and Infrastructure Security Agency, stated that in the event of a Chinese invasion of Taiwan, the CCP may target "multiple U.S. gas pipelines; the mass pollution of our water systems; the hijacking of our telecommunications systems; the crippling of our transportation nodes—all designed to incite chaos and panic across our country . . . ."[6] In testimony before the Committee on Homeland Security on April 27, 2023, Director Easterly emphasized that DHS must be able to help mitigate, recover, and "have the resilience to get our nation back up and running again if there is a major [cyber] attack [from China]".[7] To prepare for potential threats to our critical infrastructure, DHS must assess its current capabilities to combat them, and make clear to Congress what resources and authorities DHS may need to do so.

Given the security risks associated with the extensive use of Chinese-manufactured cranes that threaten to undermine our national security and to assist the Committees with their oversight of operational technology in U.S. port infrastructure, please provide a full production in response to the April 3, 2023 Committee on Homeland Security letter, and the following documents and information as soon as possible, but no later than 5:00 p.m. on May 24, 2023:

1. All documents and communications, including but not limited to memoranda, intelligence bulletins, threat assessments, and briefing materials referring or relating to ZPMC and/or any other Chinese-based crane manufacturer for the period of January 1, 2000, to the present;

---

[4] *Id.*
[5] Maggie Miller, *What it Will Look Like if China Launches Cyberattacks in the U.S.*, POLITICO, Apr. 16, 2023, https://www.politico.com/news/2023/04/16/chinese-hackers-military-taiwan-invasion-00092189.
[6] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, *CISA Director Easterly Remarks at Carnegie Mellon University* (Feb. 27, 2023), *https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university.See also*: *Annual Threat Assessment of the U.S. Intelligence Community*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE (Feb. 6, 2023), www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.
[7] *See CISA 2025: The State of American Cybersecurity from CISA's Perspective*. Hearing Before the H. Comm. on Homeland Sec., 118th Cong. (April 27, 2023) (statement of Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency), https://homeland.house.gov/tomorrow-at-2pm-garbarino-to-lead-subcommittee-hearing-with-cisa-director-jen-easterly/.

2. All documents sufficient to describe the steps DHS has taken to identify, assess, and mitigate the risks associated with Chinese software and operational technology in U.S. ports;

3. All documents sufficient to describe any existing DHS collaborations or partnerships with private sector entities, state and local governments, and international partners to address the issue of Chinese software and operational technology in U.S. ports;

4. All documents sufficient to describe any training or education initiatives provided to DHS personnel, state and local governments, and private sector entities to identify and respond to the risks associated with Chinese software and operational technology in U.S. ports;

5. All documents sufficient to describe any and all outreach efforts made to foreign allies and partners to raise awareness about the risks of Chinese software and operational technology in their ports;

6. All documents listing any and all known or suspected incidents of cyber-attacks or espionage linked to Chinese software and operational technology in U.S. ports from January 1, 2000, to the present;

7. All documents sufficient to show an analysis of the potential long-term consequences of continued reliance on Chinese software and operational technology in U.S. port infrastructure and any potential threats to U.S. national security posed by the presence of Chinese software and operational technology in U.S. ports;

8. All documents sufficient to describe how DHS coordinates with other federal agencies, such as the Department of Commerce, the Department of Defense, and the Committee on Foreign Investment in the United States (CFIUS), to address the issue of Chinese software and operational technology in U.S. ports; and

9. All documents sufficient to describe ongoing research and development initiatives within DHS or in collaboration with external partners, aimed at creating secure alternatives to Chinese software and operational technology in U.S. ports.

Additionally, please provide a staff-level briefing to the committees as soon as possible, but no later than May 31, 2023.

An attachment contains instructions for responding to this request. To the maximum extent possible, provide unclassified responses to these requests. Any classified information provided in response to this letter should be provided under separate cover.

Please contact China Select Committee Majority staff at (202) 226-9678 and Homeland Security Committee Majority staff at (202) 226-8417 with any questions about this request.

The House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party has broad authority to "investigate and submit policy recommendations on the status of the Chinese Communist Party's economic, technological, and security progress and its competition with the United States" under H. Res. 11.

Under 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 attention to this important matter and your prompt reply.

Sincerely,

Mark E. Green, M.D.
Chairman
Committee on Homeland Security

Mike Gallagher
Chairman
Select Committee on China

Carlos A. Gimenez
Chairman
Subcommittee on Transportation and Maritime Security

Andrew R. Garbarino
Chairman
Subcommittee on Cybersecurity and Infrastructure Protection

Dan Bishop
Chairman
Subcommittee on Oversight, Investigations, and Accountability

August Pfluger
Chairman
Subcommittee on Counterterrorism, Law Enforcement, and Intelligence

Encl.

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

The Honorable Raja Krishnamoorthi, Ranking Member
Select Committee on China

The Honorable Shri Thanedar, Ranking Member
Subcommittee on Transportation and Maritime Security

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

The Honorable Glenn Ivey, Ranking Member
Subcommittee on Oversight, Investigations, and Accountability

The Honorable Seth Magaziner, Ranking Member
Subcommittee on Counterterrorism, Law Enforcement, and Intelligence