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

April 3, 2023

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

Dear Secretary Mayorkas:

We write today to express our concern about existing vulnerabilities at our nation's maritime ports. We are particularly concerned about technology employed by Chinese-manufactured cranes operating in U.S. ports, which significantly increases the cybersecurity risk to business operations systems and terminal industrial control systems.

To address these concerns, the Committee on Homeland Security is conducting oversight of vulnerabilities in our nation's maritime ports and the Department of Homeland Security's (DHS) resilience strategies to address them. As you know, DHS is the lead federal agency responsible for our nation's maritime port security and cybersecurity. America's supply chain and economic security are largely dependent on maritime ports, which help facilitate $5.4 trillion worth of commercial and military goods, annually.[1]

Maritime port security is vital to our national security. On November 30, 2022, a bicameral group of Members sent a letter to President Biden urging action and decisive response to the threats posed by China at our nation's ports.[2] We renew that call. Among other issues, we find troubling that Chinese-made cranes manufactured by Shanghai Zhenhua Heavy Industries Co., also known as ZPMC, are utilized in 80 percent of U.S. ports.[3]

As described recently in the *Wall Street Journal*, these cranes "contain sophisticated sensors that can register and track the provenance and destination of containers, prompting concerns that China could capture information about materiel being shipped in or out of the country to support U.S. military operations around the world."[4] If this report is correct, data

[1] *Exports, Jobs & Economic Growth*, American Association of Port Authorities, https://www.aapa-ports.org/advocating/content.aspx?ItemNumber=21150.
[2] Letter from Sen. Tom Cotton et al., to President Joseph R. Biden (Nov. 30, 2022) *available at* https://www.cotton.senate.gov/imo/media/doc/logink.pdf.
[3] Aruna Viswanatha, Gordon Lubold, and Kate O'Keeffe, *Pentagon Sees Giant Cargo Cranes as Possible Chinese Spying Tools*, WALL STREET J., Mar. 5, 2023, https://www.wsj.com/articles/pentagon-sees-giant-cargo-cranes-as-possible-chinese-spying-tools-887c4ade.
[4] *Id.*

collection of military shipments and visibility into our nation's defense industrial base presents an enormous threat to our military strategic competitive advantages.

Even more concerning, the parent company of ZPMC, China Communications Construction Co. (CCCC), is a leading Belt and Road Initiative[5] contractor with close ties to the People's Liberation Army (PLA) and participates in military civil fusion.[6] In July 2018, the CCCC's "military-civilian fusion office signed a 'strategic cooperation' agreement with the PLA's Naval Logistics Academy, pledging to collaborate on matters related to the development of maritime defense projects, theoretical research and big-data, among other areas."[7] ZPMC's relationship with CCCC is disconcerting, especially given the prevalence of ZPMC cranes in U.S. ports.

Furthermore, if an adversary exploits the operational technology (OT) system of these cranes, port operations could completely shut down, suspending all commercial activity which would also disrupt our nation's military and commercial supply chains.[8] According to a former top U.S. counterintelligence official, "[c]ranes can be the new Huawei."[9] Any potential port shut down could create catastrophic economic and security consequences. These vulnerabilities could provide opportunities to near-peer nation-state adversaries, such as China, to cripple our economy from behind a computer screen.

To assist the Committee in its oversight of DHS's maritime port security efforts, please schedule a briefing to Committee staff on maritime port security with a focus on maritime port cybersecurity as well as the vulnerabilities ZPMC's cranes in U.S. ports may pose, as soon as possible, but no later than 5:00 p.m. on April 14, 2023. In addition, please provide the following documents and information as soon as possible, but no later than 5:00 p.m. on April 17, 2023:

1. All documents and communications referring or relating to security vulnerabilities ZPMC or other foreign-manufactured cranes employed at U.S. ports pose to U.S. maritime ports from January 1, 2000 to the present;

2. Documents sufficient to show the risk assessment and emergency preparedness measures in place by sector risk management agencies (SRMAs) as directed by the FY21 National Defense Authorization Act for the Transportation System Sector, specifically as it relates to the maritime transportation sector;

---

[5] *The Belt and Road Initiative (BRI) is central to China's primary foreign policy strategy. The BRI aims to spread Chinese economic, political, and military influence by investing in critical infrastructure projects in Africa, Asia, the Middle East, Europe, and Latin America, focusing on developing nations.*
[6] *Supra* note 2.
[7] Kate O'Keeffe and Chun Han Wong, *U.S. Sanctions Chinese Firms and Executives Active in Contested South China Sea*, WALL STREET J., Aug. 26, 2020, https://www.wsj.com/articles/u-s-imposes-visa-export-restrictions-on-chinese-firms-and-executives-active-in-contested-south-china-sea-11598446551?mod=Searchresults_pos1&page=1&mod=article_inline.
[8] *Supra* note 2.
[9] *Id.*

3. Documents sufficient to show the United States Coast Guard's (USCG) Maritime Cyber Readiness Branch (MCRB) standard operating procedures to assess, address, and mitigate cybersecurity risks to maritime ports;

4. Documents sufficient to show how DHS, including the USCG, engages with the maritime port industry, including private companies, about cybersecurity threats;

5. A document sufficient to show the percentage of private maritime transportation companies that voluntarily report cybersecurity incidents to DHS;

6. A document sufficient to show the average response time of DHS, including the Cybersecurity and Infrastructure Security Agency (CISA) and USCG, for reported maritime port cybersecurity incidents; and

7. Documents sufficient to show which private companies received Federal Emergency Management Agency (FEMA) Port Security Grant program funding for FY20, FY21, FY22, and FY23 and how awardees utilized grant dollars for those fiscal years.

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. 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 House Rule X, 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."

Thank you for your prompt attention to this important matter.

Sincerely,

MARK E. GREEN, MD
Chairman

DAN BISHOP
Chairman
Subcommittee on Oversight,
Investigations, and Accountability

CARLOS GIMENEZ
Chairman
Subcommittee on Transportation
and Maritime Security

ANDREW GARBARINO
Chairman
Subcommittee on Cybersecurity
and Infrastructure Protection

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

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

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

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