



Congress of the United States
House of Representatives
Washington, DC 20515-0906

January 22, 2025

The Honorable Admiral Kevin E. Lunday
Acting Commandant
United States Coast Guard
2703 Martin Luther King Jr. Avenue SE
Washington, D.C. 20593

Dear Admiral Lunday:

We write to raise significant concerns about the national security risks posed by state-owned enterprises from the People's Republic of China (PRC) operating within the U.S. Marine Transportation System (MTS). Notably, China COSCO SHIPPING Corporation Limited, COSCO SHIPPING (North America) Inc., and Cosco SHIPPING Finance Co., Ltd. (collectively, "COSCO SHIPPING"), were recently added to the Department of Defense's list of Chinese Military Companies¹ pursuant to Section 1260H of the National Defense Authorization Act of 2021.² This designation identifies these entities as contributors to the PRC's defense industrial base,³ while underscoring COSCO SHIPPING's integral role as a key facilitator in advancing the PRC's military-civil fusion strategy.⁴

Given the PRC's track record of exploiting commercial assets for intelligence and military purposes, COSCO SHIPPING's expansive operations at major U.S. ports present significant national security concerns, including espionage, cyber intrusions, sabotage, and supply chain disruptions. These concerns are amplified by COSCO SHIPPING's substantial control over global container traffic and its proximity to U.S. critical infrastructure. Moreover, if public reports are accurate, COSCO SHIPPING vessels, like many other PRC state-owned merchant ships, frequently have Chinese Communist Party (CCP) political commissars embedded amongst their crews, further demonstrating the CCP's direct influence over these operations.⁵ The company's documented ties to the People's Liberation Army (PLA),⁶ which, in part, warranted its inclusion on the Department of Defense's Section 1260H list, only compounds

¹ Notice of Availability of Designation of Chinese Military Companies, 90 Fed. Reg. 1105, (Jan. 7, 2025).

² National Defense Authorization Act of 2021, Sec. 1260H(b)(2).

³ *Id.*, Sec. 1260H(d)(1)(B)(i)(I), (ii).

⁴ U.S. Dep't of Defense, *Military and Security Developments Involving the People's Republic of China*, (2023), <https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF>.

⁵ Conor M. Kennedy, *China Maritime Report No. 40: Onboard Political Control - The Ship Political Commissar in Chinese Merchant Shipping*, U.S. Naval War College Digital Commons, Aug. 12, 2024, <https://digital-commons.usnwc.edu/cmsi-maritime-reports/40/>.

⁶ *Id.*

the potential threats to the United States.⁷ Permitting vessels and personnel affiliated with COSCO SHIPPING to operate within U.S. ports without adequate safeguards exposes our nation to unacceptable risks, particularly during times of increased geopolitical tension.

As the lead federal agency for maritime security, the U.S. Coast Guard (USCG) must take decisive action to mitigate these risks. Achieving this goal will require a thorough assessment and strengthening of current USCG protocols for screening vessels, owners, and crew members associated with COSCO SHIPPING and other entities linked to the PLA or the PRC's security and intelligence services. The USCG must prioritize the integration of both classified and unclassified intelligence, strengthen interagency coordination and collaboration, and leverage advanced technological solutions to enhance its ability to detect and deter emerging threats.

In particular, the submission of Advance Notice of Arrival (ANOVA) data represents a key opportunity to identify and mitigate threats before foreign-flagged vessels enter U.S. waters. It is essential that biographical information for all foreign mariners, particularly those from the PRC and other high-risk countries, undergo comprehensive scrutiny utilizing the complete range of classified and unclassified data resources accessible to the U.S. government. Finally, the vetting process must be consistent and comprehensive across all U.S. ports to avoid creating gaps in security that the CCP could exploit.

Considering the seriousness of these concerns and in furtherance of our oversight responsibilities, we request a written response to the following questions as soon as possible, but no later than 5:00 p.m. on February 5, 2025:

1. What specific protocols does the USCG have in place to vet the biographic data of foreign mariners submitted through the ANOVA process?
 - How does the USCG ensure the accuracy of the information provided by foreign mariners, particularly those affiliated with entities linked to foreign adversaries such as COSCO SHIPPING?
 - Are there additional security measures applied to mariners from high-risk countries or companies with ties to the PLA or the PRC's security and intelligence services?
2. What classified and unclassified datasets are used by the USCG to vet foreign mariners, vessel owners, and operators?
 - Are these datasets maintained on Non-classified Internet Protocol Router (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), or Joint Worldwide Intelligence Communications System (JWICS) networks?
 - How frequently are these datasets updated to ensure relevancy, and what safeguards are in place to ensure their integrity and security?
3. Is the vetting process for foreign mariners and vessels consistent across all USCG Captain of the Port Zones?

⁷ *Id* at 1.

- If discrepancies exist, why are there variations in screening protocols, and how does the USCG mitigate the risk of security gaps at certain U.S. ports?
4. Is the USCG's vetting and screening process for foreign vessels and mariners fully automated, partially automated, or primarily manual?
 - What plans, if any, does the USCG have to improve the automation of these processes to ensure more timely and efficient screening?
 - How does the USCG balance the need for speed and accuracy in its vetting process, especially during periods of high vessel traffic?
 5. Does the USCG rely on any foreign-owned or third-party data systems to conduct vetting and screening operations?
 - If so, what measures are in place to ensure that these systems cannot be compromised by foreign adversaries, and what safeguards are implemented to protect U.S. data from espionage, cyberattacks, or sabotage?
 6. Who within the USCG is responsible for monitoring the movements and activities of foreign-crewed vessels before, during, and after their port calls in the United States?
 - How does the USCG ensure continuous monitoring of high-risk vessels, such as those affiliated with state-owned enterprises like COSCO SHIPPING?
 - Are there any gaps in monitoring capabilities that need to be addressed?
 7. What specific tools, technologies, and platforms does the USCG utilize to detect potential security threats posed by foreign vessels, mariners, and terminal operators?
 - How does the USCG use these tools to identify anomalies in vessel behavior, unauthorized access to critical port infrastructure, or potential cyber threats?
 8. How does the USCG coordinate with other federal agencies, including, but not limited to, the Department of Homeland Security, the Department of Defense, the Federal Bureau of Investigation, and Office of the Director of National Intelligence, to address maritime security threats posed by foreign-owned vessels and shipping companies?
 - What formal mechanisms, joint operations, or intelligence-sharing agreements are in place to ensure timely and effective interagency coordination? Please provide specific details for each mechanism, joint operation, or agreement.
 - Specific to vessel screening, does the USCG provide other members of the Intelligence Community (IC) the chance to participate in the vetting process? Does this happen at the national or local level? What procedures are in place to guarantee that other IC members can flag a particular vessel for an offshore security boarding by the USCG?
 9. Has the USCG conducted *any* risk assessments specific to COSCO SHIPPING operations at or between U.S. ports?
 - If so, what were the findings of these assessments, and what specific security measures have been implemented to address the risks associated with COSCO

The Honorable Admiral Kevin E. Lunday

January 22, 2025

Page 4

SHIPPING's presence in the U.S. MTS? For each assessment, please identify the title and scope, the start and completion date, and a summary of the specific findings and recommendations.

Additionally, we request that the USCG provide a classified briefing to Committee on Homeland Security and China Select Committee staff by no later than February 12, 2025.

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

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

Thank you for your attention to this important matter and your prompt reply.

Sincerely,



MARK E. GREEN, M.D.
Chairman
Committee on Homeland Security



JOHN MOOLENAAR
Chairman
Select Committee on the CCP



CARLOS A. GIMENEZ
Chairman
Subcommittee on Transportation and
Maritime Security
Committee on Homeland Security



DUSTY JOHNSON
Member of Congress

Encl.

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

The Honorable Raja Krishnamoorthi, Ranking Member
Select Committee on the CCP

The Honorable Admiral Kevin E. Lunday
January 22, 2025
Page 5

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