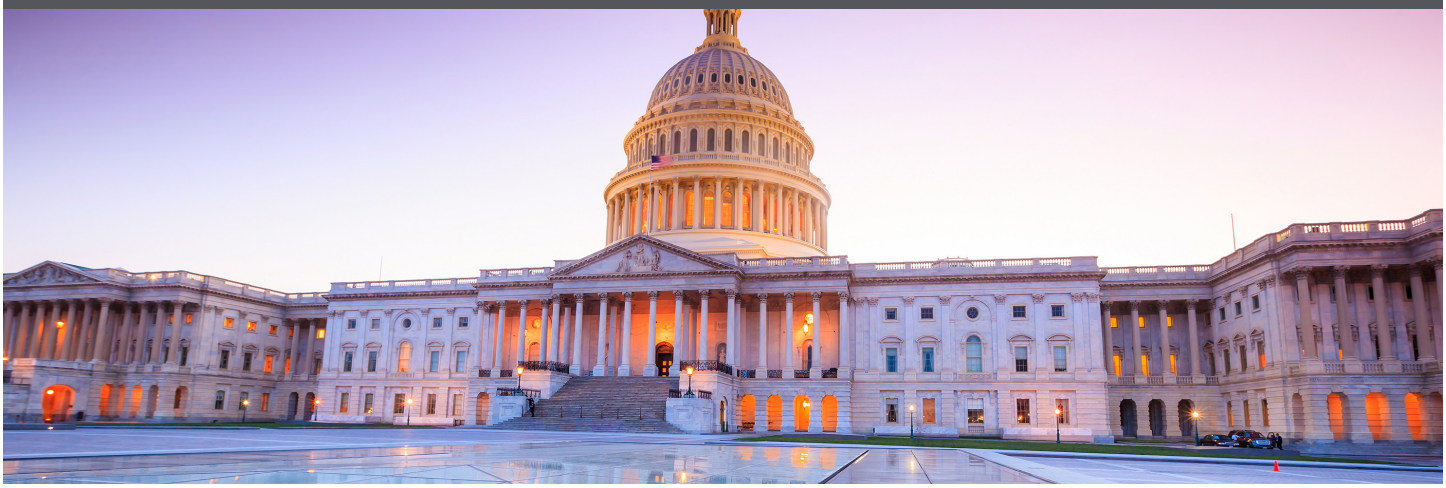
BLANKROME
Government Relations LLC

Port and Cybersecurity



MARCH 7, 2024

White House and Coast Guard Warn of Chinese Cranes at U.S. Ports

President Biden recently signed an Executive Order ("EO") designed to, according to the Administration's Fact Sheet, "bolster the security of the nation's ports, alongside a series of additional actions that will strengthen maritime cybersecurity, fortify our supply chains, and strengthen the United States industrial base."

This February 21, 2024, move by the Biden Administration comes as cybersecurity concerns continue to be raised following various attacks on logistics systems throughout the United States. Administration officials have voiced concern that more than 200 ship-to-shore cranes at U.S. ports are manufactured by China and can be serviced and programmed remotely. In early 2023, defense officials raised concerns about possible spying efforts being conducted by Chinese manufacturer Shanghai Zhenhua Heavy Industries Co. ("ZPMC"), which controls much of the global and U.S. markets for these cranes. This concern for cybersecurity was also validated by the disruption of Japan's Port of Nagoya, which was impacted by a ransomware attack last summer. This announcement comes after the Biden Administration warned in early February that a state-sponsored group of Chinese hackers, known as Volt Typhoon, has for years been working to access critical maritime, aviation, mass transit, and pipeline operations in what the United States described as an effort of "prepositioning themselves on IT networks" ahead of a possible effort to disrupt critical functions.

As part of the actions included in the EO, the U.S. Coast Guard ("USCG") published a Notice of Proposed RuleMaking ("NPRM") that will provide baseline cybersecurity requirements to protect the Maritime Transportation System ("MTS") from cyber threats. The agency is inviting public comment on this proposed rule through April 22, 2024.

EXECUTIVE ORDER HIGHLIGHTS

Coast Guard Authority Increased by:

- Amending multiple sections of Part 6, Title 33 of the Code of Federal Regulations ("CFR") to include "cyber incidents" in the list of threats posed to the MTS.
- Incorporating the definition of "incident" from 44 U.S.C. 3552(b)(2).
- Adding a new reporting requirement to mandate that a cyber incident involving "any vessel, harbor, port, or waterfront facility" must be reported to the Federal Bureau of Investigation ("FBI"), the Cybersecurity and Infrastructure Security Agency ("CISA"), and the captain of the port. This new reporting requirement adds to the already existing obligations of "the master, owner, agent, or operator of a vessel or waterfront facility" to prevent sabotage and subversive activity.

- Extending the authority of the Coast Guard over cybersecurity threats. The Coast Guard may now take possession or control of vessels presenting a cybersecurity threat.

Distributed Private Maritime Cybersecurity Directive:

- The Coast Guard privately distributed Maritime Security ("MARSEC") Directive 105–4 on cyber risk management actions for ship-to-shore cranes manufactured by the People's Republic of China located at U.S. commercial strategic seaports. The directive is targeted towards "owners or operators of ship-to-shore ("STS") cranes manufactured by People's Republic of China ("PRC") companies." Owners and operators of these cranes must acknowledge the directive and take a series of actions on these cranes and associated information technology ("IT") and operational technology ("OT") systems. Considering the sensitivity of the information provided in the directive, the directive has not been distributed to the public.

Increased Investment:

- The Administration will invest over $20 billion, including through grants, in U.S. port infrastructure over the next five years through the President's Investing in America Agenda, including the Bipartisan Infrastructure Law and the Inflation Reduction Act. As a result, PACECO Corp., a U.S.-based subsidiary of Mitsui E&S Co., Ltd. (Japan), is planning to onshore U.S. manufacturing capacity for its crane production.

COAST GUARD'S NOTICE OF PROPOSED RULEMAKING ("NPRM") HIGHLIGHTS

- The Coast Guard published proposed rules at once following the signing of the EO. The rules use cybersecurity frameworks established by CISA and the National Institute of Standards and Technology ("NIST") to address cybersecurity and governance issues pertaining to ports.

- Owners and operators of U.S.-flagged vessels and facilities in U.S. waters and on the Outer Continental Shelf ("OCS") will be required to develop and submit a cybersecurity plan for review and approval by the USCG.

- Owners and operators must conduct cybersecurity drills and exercises to test capacity to respond to cybersecurity attacks.

- Owners and operators must implement cybersecurity measures like training, data security, and device security.

- MTS stakeholders must report cyber incidents to the USCG within 24 hours after discovery.

- These cybersecurity requirements will be phased in. The first compliance date will be the second annual audit of the existing approved Vessel Security Plan, OCS facility Security Plan, or Facility Security Plan after the effective date of the final rule.

- The agency is inviting public comment on this proposed rule through April 22, 2024.

HOMELAND SECURITY HEARING

Following these actions, the House Homeland Security Subcommittee on Transportation and Maritime Security held a hearing entitled, "Port Cybersecurity: The Insidious Threat to U.S. Maritime Ports," on February 29, 2024, where witnesses were asked about the recent actions taken to combat threats to U.S. ports' infrastructure, specifically ship-to-shore cranes.

The hearing's witnesses, which included Rear Admiral Wayne Arguin, who serves as the Assistant Commandant for Prevention Policy with the USCG, as well as other officials from the USCG, the U.S. Transportation Command ("TRANSCOM"), and the Department of Homeland Security, were pressed by representatives on the nation's infrastructure reliance on China. Witnesses expressed concern about the extent of Chinese manufacturing presence in critical U.S. port operations but were all in agreement that Biden's Executive Order would bolster their ability to execute port security efforts by explicitly addressing cyber threats.

"What the EO really does, again, is allow a captain of the port, if it's determined that there is a threat or there has been some disruption because of a cyber intrusion, to take action to secure a crane or secure a terminal until such time that the operator, maybe with our assistance or at least with our validation, takes action to secure that particular node of the system," RDML Arguin stated at the hearing.

In general, Democratic and Republican members of the Subcommittee, as well as the witnesses, shared similar concerns about threats posed by China on the nation's maritime ports, but were also all in agreement that Biden's EO, along with the Coast Guard's Notice of Proposed Rulemaking, are great steps forward in strengthening the nation's supply chain and bolstering the security of our ports. They also offered to support the Coast Guard in implementing the new rules.

For more information or assistance, contact C.J. Zane, Stephen C. Peranich, Joan M. Bondareff, Scott Moore, Addison Sheppard, or another member of the Blank Rome Government Relations LLC team.

C.J. Zane
202.772.5975 | cj.zane@blankrome.com

Stephen C. Peranich
202.772.5924 | stephen.peranich@blankrome.com

Joan M. Bondareff
202.772.5911| joan.bondareff@blankrome.com

Scott Moore
202.420.2255 | scott.moore@blankrome.com

Addison Sheppard
202.420.2783 | addison.sheppard@blankrome.com

Resources:

- News Article — Bloomberg Government (bgov.com)
- US Coast Guard proposes cybersecurity regulations for maritime sector, seeks feedback by Apr. 22 - Industrial Cyber
- Biden administration issues Executive Order and takes action to enhance maritime cybersecurity | Data Protection Report
- Biden executive order on port cybersecurity targets China-made cranes (cnbc.com)

© 2024 Blank Rome Government Relations LLC. All rights reserved. Please contact Blank Rome Government Relations for permission to reprint. Notice: The purpose of this update is to identify select developments that may be of interest to readers. The information contained herein is abridged and summarized from various sources, the accuracy and completeness of which cannot be assured. This update should not be construed as legal advice or opinion, and is not a substitute for the advice of counsel.