The Maritime Executive
INTELLECTUAL CAPITAL FOR LEADERS

USCG Instructs Owners of Chinese STS Cranes to Take More Security Steps

Critics highlight that China ships the cranes fully assembled to ports around the world

Published Nov 21, 2024 8:09 PM by The Maritime Executive

The U.S. Coast Guard this week reported it has made available a further cyber risk management directive for all the owners of Chinese-made maritime ship-to-shore cranes. It is in addition to a previously released MARSEC Directive in February 2024 after President Joe Biden instructed that steps were required to protect U.S. port infrastructure from cyber dangers from the Chinese.

The notice of availability of the further directive said the owners and operators of the canes should immediately contact their local Coast Guard Captain of the Port or District Commander. Because the directive contains "security-sensitive information," USCG says it cannot be made available to the general public.The new directive is dated November 13, 2024.

The alert highlights the well-known fact that STS cranes manufactured in China make up the largest share of the global ship-to-shore crane market. USCG said these cranes account for nearly 80 percent of the STS cranes at U.S. ports.

"By design, these cranes may be controlled, serviced, and programmed from remote locations, and those features potentially leave STS cranes manufactured by PRC companies vulnerable to exploitation, threatening the maritime elements of the national transportation system," wrote the USCG announcing the new directive.

The alert goes on to state that additional measures are necessary to prevent a "transportation security incident in the national transportation system" due to the prevalence of STS cranes manufactured in China. It points to "threat intelligence related to the PRC's interest in disrupting U.S.

critical infrastructure, and the built-in vulnerabilities for remote access and control of these STS cranes."

President Biden placed additional authority with USCG to manage cybersecurity threats and required additional analysis of the situation at the ports. Specifically, he cited the crane threat and announced initiatives to reshore crane manufacturing capability in the United States. In addition, KRONE during the summer highlighted its efforts at manufacturing cranes as an alternative to China's Shanghai Zhenhua Heavy Industries (ZMPC) which claims a 70 to 80 percent worldwide market share.

The American Ports Association initially dismissed the threat after reports in 2023 and continues to assert that there are no examples of cyber breaches or interference with operations. The initial reports associated the cranes with spying but it was highlighted that there was no data on the crane to the nature of the cargo or the operations.

USCG now points to the potential to interrupt operations. This comes after media reports surfaced in March 2024 that modems had been found installed on the cranes. The House Homeland Security Committee asserted it had discovered "a pattern of suspicious device installations" fueling the fears of potential cybersecurity risks.

The United States Trade Representative joined in the debate announcing in September that it would accept the Biden administration recommendation and impose a 25 percent tariff on Chinese-made STS cranes. The ports' association complained of the added expense and said ports were being penalized with no clear alternative. The tariffs were amended so that orders placed prior to May 2024 and delivered by 2026 would not have the tariff imposed.

Congressional investigations recommended that ports disable the modems and communications capabilities immediately on the cranes. They also called for steps to bar Chinese cranes and the logistics software developed in China to protect U.S. ports.