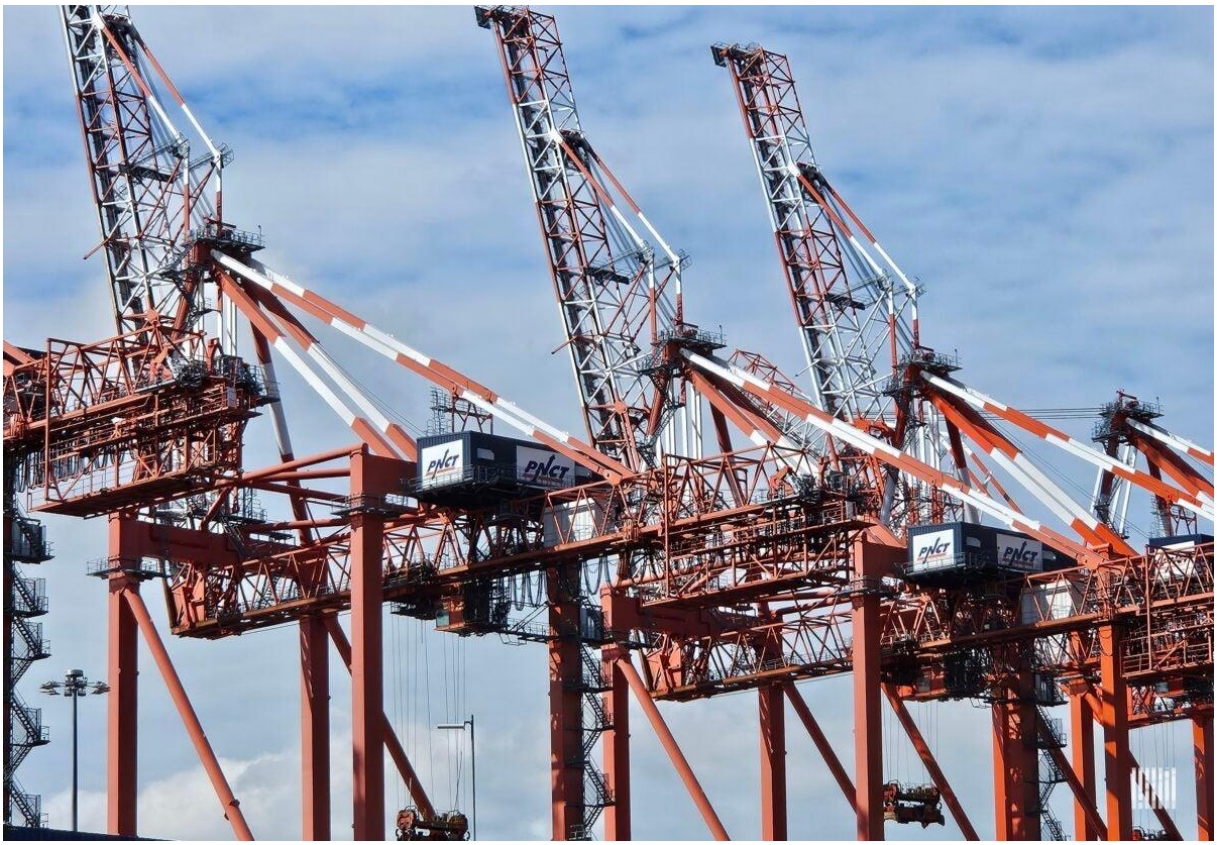
US warns of cyberthreat from China container cranes

Coast Guard directive adds systems risk warning

Stuart Chirls

Wednesday, November 27, 2024



(Photo by Stuart Chirls/FreightWaves)

The U.S. Coast Guard issued an additional warning to American ports of potential security risks posed by container cranes made in China.

The new MARSEC Directive 105-5 sets out additional cyber risk management requirements for ship-to-shore cranes made by Chinese companies.

The directive follows a previous mandate for security measures issued in February.

The new directive in part states that “built-in vulnerabilities for remote access and control of these STS cranes, combined with intelligence regarding China’s interest in disrupting U.S. critical infrastructure, necessitate immediate action,” the Coast Guard said in a release.

The agency said some cranes are equipped with control technology that could enable China to gain remote access to ports, terminals and computer-based systems.

China cranes are in use at about 80% of U.S. ports. The leading maker is state-owned Shanghai Zhenhua Heavy Industries Co. Ltd., which has 200 cranes in operation at American container hubs.

The three-level MARSEC system is used to communicate possible security threats to maritime shipping.

President Joe Biden earlier this year signed an executive order stipulating that billions of dollars in infrastructure funding for port upgrades replace the cranes with ones made in America.

Under the directive, port and terminal operators, crane owners, and other parties involved in the installation, maintenance and support of Chinese-manufactured STS cranes are required to contact their Coast Guard District commander or captain of the port to obtain a copy of the clearance-sensitive directive.

*Find more articles by Stuart Chirls **here**.*