What 4 Cyber Protection Actions Mean For Marine Transport

By **Sean Pribyl, Shardul Desai and Jameson Rice** (June 17, 2024)

Sean Pribyl

Shardul Desai

Jameson Rice

Maritime trade is essential to America's economic viability and national security interests. The U.S. Marine Transportation System — comprising an intricate system of ports, terminals, vessels, waterways and land-based facilities — reportedly supports $5.4 trillion worth of economic activity each year and nearly 95% of cargo entering the U.S.[1]

Not only is maritime transportation critical for the movement of trillions of dollars of economic goods into the U.S. supply chain, it is also essential for the U.S. military's movement of goods to defend American's vital interests. As such, the Marine Transportation System has long been considered a part of the U.S.' critical infrastructure sector.[2]

Over the past three decades, the maritime industry has increasingly implemented internet-connected technologies and digital systems intended to improve commercial vessel and port facility operations, such as those used for the movement of cargo and ship navigation.

However, these digital interconnections have introduced cybersecurity risks, including the threat of ransomware attacks that can disrupt operations, unauthorized access to Marine Transportation System controls and navigation systems, espionage in supply chain practices and behaviors, and theft of port operations' trade secrets.

On Feb. 21, the White House **announced** a series of actions to confront these and other maritime cyber threats.[3]

First, the Biden administration said it will invest over $20 billion in U.S. port infrastructure over the next five years, including rebuilding the U.S. manufacturing capability of ship-to-shore port cranes. In addition,

Second, the White House said that the U.S. Coast Guard would issue a maritime security directive on cyber risk management actions for Chinese-manufactured ship-to-shore cranes.

Third, President Joe Biden signed the "Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States" to enhance maritime cybersecurity that bolsters the U.S. Department of Homeland Security's authority to address maritime cyber threats.

And fourth, the Coast Guard issued a notice of proposed rulemaking that proposes new

minimum cybersecurity requirements for U.S.-flag vessels, U.S. Outer Continental Shelf, or OCS, facilities and U.S. facilities subject to the Maritime Transportation Security Act regulations.

Maritime Cyber Threats and Chinese Espionage

Ports are the entry and egress for seaborne commerce and defense, and are a critical part of the U.S. supply chain infrastructure. Thus, cyber threats to maritime facilities and assets are a national security concern.

For example, a cyberattack that shuts down port operations could lead to disruptions in domestic supply chains, with imports or exports stalled at ports, creating massive downstream shortages of goods.

These supply chain concerns are not merely theoretical. Over the last several months, multiple cyberattacks affected port and vessel operations, causing substantial economic harm.

Around Christmas 2022, the Port of Lisbon, Portugal, was the victim of a ransomware attack. Although the ransomware attack allegedly did not compromise operation activities, the port's website was down for several days, and cybercriminals demanded a $1.5 million payment to stop their release of the port's financial reports, contracts, cargo information, ship logs, crew details and other port documents.[4]

In July 2023, the LockBit ransomware group successfully shutdown Japan's largest port, the Nagoya Port, for two days causing cargo congestion.[5]

In November 2023, a cyber intrusion on the systems of DP World Australia — Australia's second-largest port operator, which manages nearly 40% of Australia's seaborne commerce — resulted in disconnection from the internet, operations being shut down for several days and cargo containers being stuck on docks.[6]

The Biden administration also recently expressed unprecedented concerns about the Chinese government's ability to infiltrate U.S. critical infrastructure.[7] Highlighting these respective cyber threats, the U.S. government has expressed increased scrutiny concerning Chinese-manufactured ship-to-shore cranes.

According to the Wall Street Journal, which has written a series of articles on the cybersecurity risks of these Chinese-manufactured port cranes, a Chinese state-owned enterprise, Shanghai Zhenhua Heavy Industries Company Ltd. makes nearly 80% of the ship-to-shore cranes in use at U.S. ports.[8]

Government officials in the Biden administration have expressed concerns of the potential threat of disruption and espionage presented by the Zhenhua cranes — especially those that can be controlled, serviced and programmed from remote locations.

Coast Guard cyber protection teams also are inspecting these Zhenhua cranes to assess cybersecurity and hunt for threats.

Coast Guard Maritime Security Directive Concerning Chinese-Manufactured Cranes

The administration clarified that it is not exploring a "rip and replace" policy that would require these Chinese-manufactured port cranes be replaced with trusted cranes.

Instead, on Feb. 23, the Coast Guard issued a maritime security directive — MARSEC Directive 105-4 — on cyber risk management actions to address the current cyber threats associated with Zhenhua cranes.[9]

This directive imposes several cybersecurity requirements on the owners and operators of the Chinese-manufactured cranes; however, the specific requirements are not being disclosed publicly for security purposes.[10]

Executive Order No. 14116

On Feb. 21, President Joe Biden issued Executive Order No. 14116 on amending regulations for safeguarding U.S. vessels, harbors, ports and waterfront facilities.

Notably, the executive order updates several regulations in Title 33 of the Code of Federal Regulations, Part 6, to explicitly address maritime cyber threats upon finding that "the security of the United States is endangered by reason of disturbances in the international relations of the United States that exist as a result of persistent and increasingly sophisticated malicious cyber campaigns against the United States, and that such disturbances continue to endanger such relations."

This follows maritime network security issues and agency responsibilities identified in the 2020 National Maritime Cybersecurity Plan.

The executive order cites Title 46 of the U.S. Code, Section 70051, commonly referred to as the Magnuson Act, which generally authorizes the president to issue regulations to safeguard vessels, harbors, ports and waterfront facilities in the U.S. against destruction, loss, or injury from sabotage or other subversive acts, accidents or similar causes.

This new order further enables the protection and security of vessels, harbors, ports and waterfront facilities by explicitly addressing cyber threats.

Among other amendments, the updated regulations provide a Coast Guard captain of the port with the authority to respond to malicious cyber activity by establishing security zones, controlling the movement of vessels that present a known or suspected cyber threat to U.S. maritime infrastructure, inspecting and searching vessels and waterfront facilities, including cyber systems and networks, as consistent with law.

The updated regulations also require facilities to correct unsatisfactory cyber conditions that may endanger the safety of a vessel, facility or harbor.

The executive order also mandates the reporting of cyber incidents. Specifically, Code of Federal Regulations Part 6.16-1 was amended to require immediate reporting of an actual or threatened cyber incident involving or endangering any vessel, harbor, port, or waterfront facility, including any data, information, network, program, system, or other digital infrastructure, to the FBI, the Cybersecurity and Infrastructure Security Agency, and the Coast Guard captain of the port, or to their respective representatives.

The reporting of cyber incidents under the executive order is a "requirement rather than a request."

The Coast Guard published Navigation and Vessel Inspection Circular 02-24 to clarify this reporting requirement. NVIC 02-24 requires cyber incidents to be reported immediately to

the FBI, Cybersecurity and Infrastructure Security Agency and the Coast Guard captain of the port.

Under the executive order, a cyber incident is defined as "an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

Marine Transportation System Cybersecurity Notice of Proposed Rulemaking

Although the Coast Guard has been addressing maritime cybersecurity as a matter of vital importance for several years, it promulgated a notice of proposed rulemaking on cybersecurity in the Marine Transportation System to establish minimum cybersecurity requirements for U.S.-flagged vessels, U.S. OCS facilities, and U.S. facilities subject to the Marine Transportation Safety Act regulations.

Foreign-flagged vessels are exempt from this proposed rule since, according to the notice, "cyber regulations for foreign-flagged vessels under domestic law may create unintended consequences with the ongoing and future diplomatic efforts to address maritime cybersecurity in the international arena."

Instead, the Coast Guard suggests that a safety management system approved under the International Safety Management Code should address foreign-flagged vessel cybersecurity. However, reporting requirements for certain hazardous conditions remain in place, which cover all foreign vessels that are bound for, or departing from, ports or places within the navigable waters of the U.S.

The notice requires regulated entities to develop cybersecurity programs that harmonize to the National Institute of Standards and Technology's cybersecurity framework.

Owners and operators of applicable U.S.-flagged vessels, U.S. facilities and OCS facilities also must develop detailed cybersecurity plans that contain the specific requirements and standards — to varying degrees.

Such requirements and standards would be added to facility security plans, OCS facility security plans and vessel security plans. The following are some of the items that must be included in the cybersecurity plan: drills and exercises, access controls, device and data security, personnel training, risk management, network segmentation and audits.

Owners and operators of applicable U.S.-flagged vessels, U.S. facilities and OCS facilities must submit their cybersecurity plan to the Coast Guard for review and approval. Moreover, the notice of proposed rulemaking requires mandatory reporting of cyber incidents to the national response center without delay.

Notably, in the notice, a cyber incident is defined more narrowly than in the Coast Guard's NVIC 02-24.

Under the notice, a cyber incident is "an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system or actually jeopardizes, without lawful authority, an information system."

Unlike the NVIC 02-24 definition, the notice's definition does not include an occurrence that "immediately" jeopardizes or violations of the law or a security policy. Owners and operators

of applicable U.S.-flagged vessels, U.S. facilities and OCS facilities must maintain a cyber incident response plan and test the plan through annual tabletop exercises.

The notice of proposed rulemaking sought public comments on whether the Coast Guard should use and define the term "reportable cyber incident" to limit cyber incidents that trigger reporting requirements, require cyber incident reporting to the Cybersecurity and Infrastructure Security Agency in harmonization with the Cyber Incident Reporting for Critical Infrastructure Act and amend the definition of "hazardous condition."

The notice's comment period closed on May 22. Once final rules are adopted, the Coast Guard is proposing an implementation period of 12 to 18 months.

Key Takeaways

The Biden administration's above-described actions reflect its continued efforts to secure the country's supply chains and strengthen the cybersecurity of our nation's critical infrastructure. In the interconnected economy of the U.S., these efforts are necessary to protect against cyber threats and espionage.

Nevertheless, the administration's actions create new risks, legal liabilities, and increased costs for owners and operators of applicable U.S.-flagged vessels, U.S. facilities and OCS facilities.

Owners and operators of applicable U.S.-flagged vessels, U.S. facilities and OCS facilities also should be mindful that cyber incident reporting laws often create legal liabilities for regulated entities. Such owners and operators may face challenges in determining whether an incident is reportable and when notification requirements are triggered.

Although the timing requirements in the regulations — i.e., "immediate" and "without delay" — reflect a desire to have incidents reported as close to discovery as possible, some internal investigative efforts with the company's legal counsel will be necessary and advisable to determine whether the incident is reportable in the first instance.

Thus, owners and operators of applicable U.S.-flagged vessels, U.S. facilities and OCS facilities should develop incident response plans and test the plans' effectiveness for responding to and investigating incidents quickly, and reporting incidents promptly.

A component of effective incident response involves coordinating with incident response counsel. As adverse publicity and litigation often follow data breaches, so internal investigations of cyber incidents, and the reporting cyber incidents to regulators and law enforcement, should be appropriately tailored to avoid inadvertent waiver of privilege or the creation of unnecessary litigation risks.

Sean T. Pribyl is a partner at Holland & Knight LLP. He previously served as a U.S. Coast Guard officer and attorney, and a U.S. Department of Justice special U.S. attorney.

Shardul Desai is a partner at the firm and a former federal prosecutor.

Jameson Rice is a partner and leader of the supply chain team at the firm.

of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] White House, Fact Sheet: Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports: https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/.

[2] Presidential Policy Directive 21: Critical Infrastructure Security and Resilience; see also CISA, Critical Infrastructure Sectors: Transportation System Sector: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sect.

[3] White House, Fact Sheet: Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports: https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/.

[4] Industrial Cyber, "Port of Lisbon targeted by LockBit ransomware hackers, website still down": https://industrialcyber.co/news/port-of-lisbon-targeted-by-lockbit-ransomware-hackers-website-still-down/#:~:text=LockBit%20has%20threatened%20the%20Port,24%20hours%20by%20paying%20%241%2C000.; Security Affairs, "Lockbit ransomware gang claims to have hacked the Port of Lisbon": https://securityaffairs.com/140137/cyber-crime/lockbit-group-port-of-lisbon.html.

[5] CPO Magazine,"Largest Japanese Port Suffered a Russian Ransomware Attack Halting Cargo Operations": https://www.cpomagazine.com/cyber-security/largest-japanese-port-suffered-a-russian-ransomware-attack-halting-cargo-operations/.

[6] The Guardian,"DP World hack: port operator gradually restarting operations around Australia after cyber-attack";The Wall Street Journal, https://www.theguardian.com/australia-news/2023/nov/13/australian-port-operator-hit-by-cyber-attack-says-cargo-may-be-stranded-for-days, "Major Australian Ports Reopen After Cyberattack Halts Operations": https://www.wsj.com/articles/dp-world-says-operations-resume-at-four-australian-ports-after-cyberattack-819f4af3.

[7] Wall Street Journal, "Chinese Hacking Against U.S. Infrastructure Threatens American Lives, Officials Say": https://www.wsj.com/politics/national-security/u-s-disables-chinese-hacking-operation-that-targeted-critical-infrastructure-184bb407, Wall Street Journal "FBI Director Says China Cyberattacks on U.S. Infrastructure Now at Unprecedented Scale"; Washington Post, "China's cyber intrusions have hit ports and utilities, officials say": https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/.

[8] Wall Street Journal, Pentagon Sees Giant Cargo Cranes as Possible Chinese Spying Tools - WSJ: https://www.wsj.com/politics/national-security/pentagon-sees-giant-cargo-cranes-as-possible-chinese-spying-tools-887c4ade.

[9] Fed. Reg. Vol. 89, No. 37 13726-27 (Feb 23, 2024).

[10] U.S. Coast Guard, "Content - Maritime Security (MARSEC) Directive 105–4...

(uscg.mil)": https://homeport.uscg.mil/Lists/Content/DispForm.aspx?ID=89335&Source=/Lists/Content/DispForm.aspx?ID=89335.