BIDEN ADMINISTRATION TAKES ACTIONS TO BOLSTER MARITIME CYBERSECURITY IN THE US MARITIME DOMAIN

Date: 15 March 2024

US Policy and Regulatory Alert

By: Luke M. Reid, Guillermo S. Christensen, Brian J. Hopkins

The maritime industry is undergoing a significant transformation that involves increased use of cyber-connected systems, coinciding with increased nation-state and cybercriminal targeting of cyber systems in ports and maritime assets. Globally, a number of ports and other maritime assets have been targeted by ransomware attacks with serious disruptions to operations. In response to this trend, the US government has announced a series of regulatory actions to combat cyber threats in the maritime domain—broadly targeted at US flag commercial vessels, waterfront facilities, and certain offshore facilities regulated by the US Coast Guard (USCG).

First, the USCG issued Maritime Security Directive 105-4 (MARSEC Directive 105-4), which requires owners and operators of ship-to-shore cranes manufactured by Chinese companies (PRC-manufactured STS cranes) to take action to address cyber threats and vulnerabilities that have been identified by the USCG. PRC-manufactured STS cranes are reportedly used at ports throughout the United States.

Second, President Biden also issued an Executive Order on 21 February 2024 (Executive Order), updating regulations in 33 C.F.R. Part 6, to explicitly address cyber threats in the US maritime domain, resulting in expanded authorities for the USCG and additional cyber incident reporting requirements for the maritime industry, among other changes.

Third, the USCG has also issued a Notice of Proposed Rulemaking (NPRM or Proposed Regulations) to update its existing maritime security regulations issued under the Maritime Transportation Act of 2002 (MTSA), 33 C.F.R. Subchapter H, with an enhanced focus on cybersecurity requirements applicable to vessels and facilities under US jurisdiction.

These initiatives, described further below, build upon and expand the existing regulatory structure for maritime cybersecurity in the United States.[1]

MARSEC DIRECTIVE 105-4—CHINESE CRANES AT US PORTS

On 21 February 2024, the USCG issued MARSEC Directive 105-4, stating that additional measures must be undertaken to address vulnerabilities and threats in connection with PRC-manufactured STS cranes.

Specifically, the USCG determined that PRC-manufactured STS cranes may be “controlled, serviced, and programmed from remote locations” and are therefore potentially “vulnerable to exploitation, threatening the maritime elements of the national transportation system.”[2] The government has not disclosed further details

regarding the basis for its determination, but the USCG has stated that additional actions are necessary due to "threat intelligence related to the PRC's interest in disrupting US critical infrastructure, and the built-in vulnerabilities" in connection with the PRC-manufactured STS cranes.[3] These threat assessments broadly align with reports of advance persistent threat actors, such as Volt Typhoon, targeting critical infrastructure.[4] The USCG has concluded that "additional measures" must be undertaken to address these cyber threats and vulnerabilities. It is estimated that PRC-manufactured STS cranes account for nearly 80% of all STS cranes[5] used across 23 major ports around the United States.[6]

As is typical, the text of the USCG's MARSEC directive which contains the "additional measures" that port owners and operators must undertake is not publicly disclosed, because it is considered Sensitive Security Information (SSI) pursuant to US law.[7] This directive took effect when issued on 21 February 2024. Owners and operators of affected US ports should immediately contact their cognizant USCG Captain of the Port to obtain access to MARSEC Directive 105-4, and follow procedures in 49 C.F.R. Part 1520 for its handling.[8] SSI may be shared with trusted advisors, such as external legal counsel, when operators may need additional guidance on how to implement the requirements.

EXECUTIVE ORDER 14116—AMENDING REGULATIONS RELATING TO THE SAFEGUARDING OF VESSELS, HARBORS, PORTS, AND WATERFRONT FACILITIES OF THE UNITED STATES, 33 C.F.R. PART 6.

On 21 February 2024, President Biden also issued Executive Order 14116, updating regulations in 33 C.F.R. Part 6, to explicitly address cyber threats in the US maritime domain. The Executive Order may be accessed here.

In general, regulations in 33 C.F.R. Part 6 provide the USCG Captain of the Port with broad authority to control and regulate vessel movement and facility operations to protect the safety and security of vessels, harbors, ports, and waterfront facilities under US jurisdiction.[9] Traditionally, the USCG has exercised this authority to mitigate risks with regard to physical security, but in accordance with the Executive Order the President has now extended this authority to specifically address and mitigate cyber risks in the maritime domain.

Among other provisions, the Executive Order added a definition for "cyber incident"[10] and established a requirement to report evidence of an "actual or threatened cyber incident" involving or endangering any vessel, harbor, port, or waterfront facility to the USCG, the Federal Bureau of Investigation, and the Cybersecurity and Infrastructure Security Agency (CISA).[11] These reporting requirements under the Executive Order are in addition to, and independent of, existing reporting requirements for other types of security incidents set forth in 33 C.F.R. § 101.305.[12] Covered entities should diligently review their incident response planning to ensure these are aligned with Executive Order's requirements.

NPRM—CYBER SECURITY IN THE MARINE TRANSPORTATION SYSTEM

Finally, the USCG has also issued Proposed Regulations to update its existing maritime security regulations that were issued under the MTSA, 33 C.F.R. Subchapter H. The Proposed Regulations are focused on expanding cybersecurity requirements applicable to US flag vessels, regulated waterfront facilities located in the United States, and certain regulated facilities on the US Outer Continental Shelf (OCS Facilities).

Existing MTSA regulations establish minimum requirements not only with regard to physical security of vessels and facilities, but also requirements related to radio and telecommunication systems, including computer systems.

The intent of the NPRM is to update and expand the MTSA regulations, placing an enhanced emphasis on cybersecurity measures in the maritime domain.

The Proposed Regulation would add minimum cybersecurity requirements to 33 C.F.R. Part 101, set out in new sections 33 C.F.R. § 101.600-665. As a general rule, if a vessel, regulated waterfront facility, or OCS Facility is currently required to have an approved security plan, then the proposed maritime cybersecurity regulations would apply.[13] The Proposed Regulation would not apply to foreign flag vessels calling on US ports.[14]

In general, the Proposed Regulation would require owners and operators of US-flagged vessels, regulated waterfront facilities, and OCS Facilities to take actions to prepare for, prevent, and respond to cyber threats and vulnerabilities.[15] Specifically, to first identify and address these cyber threats and vulnerabilities, the Proposed Regulation require the vessel or facility owner or operator to perform a cybersecurity assessment.[16] Based on the cybersecurity assessment, the owner or operator of the vessel or facility must develop and implement an effective cybersecurity plan.[17] Other key requirements set out in the proposed regulation include: designation of a qualified cyber security officer;[18] requirements for network segmentation, physical security of cyber systems, and provisions for resilience (response and recovery capabilities);[19] requirements to manage cybersecurity risks in the supply chain and the use of third-party vendors;[20] requirements for reporting cyber incidents;[21] requirements for the performance of cyber security drills and exercises;[22] requirements for the performance of cybersecurity audits;[23] and various recordkeeping related to these cybersecurity requirements.[24]

The Proposed Regulation may be accessed here. The USCG invites comments from the public including all stakeholders in the Maritime Transportation System. Comments are due by 22 April 2024.

CONCLUSION–KEY TAKEAWAYS

The maritime industry is increasingly relying on inter-connected, digital solutions for enhancing operational effectiveness, efficiency, safety, and more sustainable business operations. In response to this trend of inter-connectedness, the US government has taken significant steps to mitigate the risks associated with this digital transformation, and the cyber requirements imposed on those operating in the maritime environment have never been greater. Key takeaways regarding these initiatives include the following:

- MARSEC Directive 105-4 took effect on 21 February2024. Owners and operators of affected US ports with PRC-manufactured STS cranes should immediately contact their cognizant USCG Captain of the Port to obtain access to MARSEC Directive 105-4, to ascertain what will be required going forward.
- The reporting requirements in the Executive Order and 33 C.F.R. § 6.16-1 took effect on 21 February 2024. Owners and operators of vessels, ports, and OCS Facilities should review their vessel or facility security plans, as appropriate, to ensure the reporting policies and procedures in those plans are aligned and consistent with the new “cyber incident” reporting requirements established under the Executive Order.
- Affected maritime industry stakeholders should review the NPRM and consider providing comments to the USCG by 22 April 2024. The USCG has sought comments on several specific issues,[25] including whether any of the proposed requirements would overlap, conflict with, or duplicate existing regulatory requirements from other Federal agencies.

- Additionally, maritime stakeholders should consider reviewing the cyber aspects of their existing maritime security plans, and potentially conduct an exercise to better ascertain any gaps under the existing or Proposed Regulation.

If you have any questions regarding this alert, please contact the key team members below. Our Maritime and Cybersecurity practice leaders can provide comprehensive guidance on implementing these cybersecurity requirements and work with you to review, revise, and update incident response plans, test these via tabletop exercises, review policies and procedures, and assist with training.

FOOTNOTES

[1] The USCG exercises a broad combination of international and domestic legal authorities to implement numerous maritime security requirements for vessels and facilities operating in the US maritime domain. The existing regulations address both physical and cyber security threats to the maritime transportation system. These authorities include the MTSA and its implementing regulations at 33 C.F.R. Subchapter H; the International Ship and Port Facility Security (ISPS) Code; and the Magnuson Act of 1950, 46 U.S.C. § 70051, *et. seq*., implemented at 46 C.F.R. Part 6.

[2] Issuance of MARSEC Directive 105-4; Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies, 89 Fed. Reg. 13726 (Feb. 23 2023). MARSEC Directive 105-4 was issued by the USCG pursuant to 33 C.F.R. § 101.405 and 33 C.F.R. § 6.14-1. This notice may be accessed here.

[3] *Id.*

[4] *See* People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection | CISA

[5] *Id.*

[6] At a public announcement of these initiatives, senior White House national security officials signaled a clear emphasis on future public-private partnerships to bring STS crane manufacturing back to the United States, highlighting the Biden Administration's commitment to invest over US$20 Billion into US port infrastructure over the next five years, through the Administration's Investing in America agenda, the Bipartisan Infrastructure Law, and the Inflation Reduction Act.

[7] 33 C.F.R. § 101.405(a)(1).

[8] On the same day as these initiatives, the U.S. Maritime Administration (MARAD) released Maritime Advisory 2024-002-Worldwide-Foreign Adversarial Technological, Physical, and Cyber Influence. The Advisory updates maritime stakeholders on potential vulnerabilities to maritime port equipment, networks, operating systems, software, and infrastructure. The MARAD advisory may be accessed here.

[9] C.F.R. Part 6 was originally implemented, pursuant to the Magnuson Act of 1950, 46 U.S.C. § 70051 *et. seq*, through executive order 10173, dated 18 October 1950 (“Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States”). Executive order No. 10173, 15 Fed. Reg. 712 (Oct. 18 1950). It has been updated several times since.

[10] For purposes of reporting and application of 33 C.F.R. Part 6, a “cyber incident” is broadly defined as “an occurrence that: (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or

availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." *See* 33 C.F.R. § 6.01-8 and 44 U.S.C. § 3552(b)(2).

[11] *See* 33 C.F.R. § 6.16-1.

[12] Existing maritime security regulations in 33 C.F.R. § 101.305 require owners and operators of facilities and vessels to report breaches of security, suspicious activity, and transportation security incidents to the USCG. Given the nature of these definitions and existing reporting requirements, there will inevitably be overlap with the new requirement for reporting a "cyber incident" under 33 C.F.R. Part 6. Recognizing this reality, the USCG has issued supplemental guidance to clarify these various reporting requirements in Navigation & Vessel Inspection Circular 2-24, "Reporting Breaches of Security, Suspicious Activity, Transportation Security Incidents, and Cyber Incidents," dated 21 February 2024. This guidance may be accessed here.

[13] The proposed regulations would apply to the owners and operators of US-flagged vessels subject to 33 C.F.R. Part 104 (Maritime Security: Vessels), facilities subject to 33 C.F.R. Part 105 (Maritime Security: Facilities), and OCS facilities subject to 33 C.F.R. Part 106 (Marine Security: Outer Continental Shelf (OCS) Facilities).

[14] *See* Cybersecurity in the Marine Transportation System, 89 Fed. Reg. 13404, 13409 (proposed Feb. 22, 2024) (to be codified at 33 C.F.R. Parts 101 and 160). Most foreign flag commercial vessels calling on US ports are required to meet the ISPS Code and ISM Code, along with applicable IMO cybersecurity measures contained in MSC–FAL.1/Circ.3 and MSC Resolution 428(98).

[15] The USCG emphasizes that it is seeking to establish these minimum standards consistent with international and industry-recognized cybersecurity standards and recognizes that some owners and operators of facilities and vessels may already follow those standards. *See* NPRM at 13407.

[16] *See* 89 Fed. Reg. 13404, 13513 (proposed section 33 C.F.R. § 101.650(e)).

[17] *See id* (proposed section 33 C.F.R. § 101.655).

[18] *See id* at 13510 (proposed section 33 C.F.R. § 101.620(b)).

[19] *See id* at 13513 (proposed section 33 C.F.R. § 101.650(g)-(i)).

[20] *See id* (proposed section 33 C.F.R. § 101.650(f)).

[21] *See id* at 13510 (proposed section 33 C.F.R. § 101.620(b)(7).

[22] *See id* at 13511 (proposed section 33 C.F.R. § 101.635).

[23] *See id* (proposed section 33 C.F.R. § 101.630(f)).

[24] *See id* at 13512 (proposed section 33 C.F.R. § 101.640).

[25] This includes issues related to the definition of "reportable cyber incident" and limit the type of cyber incidents that trigger reporting requirements; whether to require certain reports identified in proposed 33 C.F.R. §§ 101.620 and 101.650 to be sent to CISA; and whether to amend the definition of "hazardous condition" in 33 C.F.R. § 160.202. *See id* at 13408.

KEY CONTACTS

LUKE M. REID
PARTNER

BOSTON
+1.617.951.9108
LUKE.REID@KLGATES.COM

BRIAN J. HOPKINS
ASSOCIATE

WASHINGTON DC
+1.202.778.9052
BRIAN.HOPKINS@KLGATES.COM

GUILLERMO S. CHRISTENSEN
PARTNER

WASHINGTON DC
+1.202.778.9095
GUILLERMO.CHRISTENSEN@KLGATES.COM