SQUIRE PATTON BOGGS

White House Issues Executive Order to Strengthen Cybersecurity at US Ports

US – March 1, 2024

On February 21, 2024, the White House issued an executive order implementing various measures to bolster the security of US ports by expanding the US Coast Guard's authority to regulate maritime cybersecurity, requiring the reporting of cyber incidents and investing in the US port critical infrastructure.

With the increasing use of connected systems in the maritime industry, these recent measures continue to demonstrate the administration's focus on improving the cybersecurity of the nation's critical infrastructure, including vessels and port facility operations, and reflects the increasing merger of economic and national security concerns in the Marine Transportation System (MTS). This particular executive order is not a one-off initiative. Rather, it is part of a broader administration strategy targeting perceived national security threats and potential threats to supply chains, including those supporting critical infrastructure.[1]

As evidenced by the May 7, 2021 ransomware attack on Colonial Pipeline, cyberattacks on US critical infrastructure, either by financially motivated criminal elements or hostile foreign actors, have the potential to significantly disrupt the economy. A 2014 cyberattack on a German steel mill caused significant physical damage, and that same year a cyberattack on Sony Pictures illustrated the crippling impact that nation-state cyberattacks can have on commercial organizations. In October 2020, the International Maritime Organization, shipping's global regulatory agency, was itself hit with a cyberattack, which underscores the fact that the maritime transportation industry is not immune to cyberthreats. In light of the fact that approximately 90% of global trade is conducted via ocean shipping according to the Organisation for Economic Co-operation and Development, protecting the country's ports is crucial to protecting the economy of the US.

Executive Order to Safeguard Against Malicious Cyber Campaigns Against US Ports

The White House issued Executive Order 14116 of February 21, 2024, expanding the authority of the US Coast Guard to safeguard against cyberthreats endangering vessels, waterfront facilities, harbors and ports, and instituting mandatory reporting of cyber incidents. The executive order demonstrates the administration's continued focus on the hardening of America's critical infrastructure against cybersecurity threats, building on the National Cybersecurity Strategy announced in March 2023.

Coast Guard Authorities

The Coast Guard is currently authorized to prevent access of, inspect and remove any person, article or thing from vessels and waterfront facilities, if necessary to prevent damage or injury.[2] The Coast Guard may further prevent the mooring of vessels, or supervise and control, vessels in such circumstances.

The executive order amends these regulations to further apply to any data, information, network, program, system or other digital infrastructure on any vessel or waterfront facility. Accordingly, the Coast Guard is authorized to prevent access of, inspect or remove "any data, information, information, network, program, system or other digital infrastructure" to secure vessels and waterfront facilities from damage or injury. The executive order instructs the Coast Guard to require vessels to address unsatisfactory cyber conditions endangering vessels, harbors or facilities prior to mooring. The Coast Guard may further supervise and control vessels to secure against cybersecurity threats. Likewise, the executive order amends existing regulations with respect to security zones to require permission in these zones prior to bringing any digital infrastructure on board a vessel.

The Coast Guard was instructed to prescribe conditions and restrictions to prevent, detect, assess and remediate any actual or threatened cybersecurity incident, as discussed below.[3]

1 In addition to the Maritime Security executive order, the White House announced on February 29, 2024 that the US Department of Commerce would be conducting an investigation into connected vehicles with software or technology that might pose a risk to US national security, and on February 28, 2024 announced and then issued Executive Order 14117 on preventing access to American's bulk sensitive personal data and US government-related data by countries of concern.

2 The Executive Order amends 33 C.F.R Part 6 and grants the Captain of the Port (COTP) authority to take various steps to ensure the safety and security to vessels, ports and waterfront facilities.

3 On February 23, 2024, the Coast Guard issued Marine Security Directive (MARSEC) 105-4 (link here). Note that "the directive contains security-sensitive information and, therefore, cannot be made available to the general public. Owners or operators of PRC-manufactured STS cranes should immediately contact their local Coast Guard COTP or District Commander for a copy of MARSEC Directive 105-4.

Cyber Incident Reporting

The executive order requires entities to report any actual or threatened cyber incidents involving vessels, harbors, ports or waterfront facilities. Reports must be made to the Coast Guard, Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA). Reporting guidelines are available at Navigation and Vessel Inspection Circular 02-24. Consistent with existing regulations, suspicious activities must also be reported (in addition to confirmed data breaches and security incidents) to enable regulatory agencies to understand the threat landscape with respect to the nation's critical infrastructure.

Coast Guard Notice of Proposed Rulemaking

As provided in the executive order, the Coast Guard issued on February 22, 2024, a Notice of Proposed Rulemaking (NPRM) to establish the minimum cybersecurity requirements for US-flagged vessels, Outer Continental Shelf (OCS) facilities and US facilities subject to the Maritime Transportation Security Act of 2002. Once implemented, these requirements will be codified in part 101 of title 33 of Code of Federal Regulations (C.F.R.), which currently contains general maritime security regulations.

Pursuant to the NPRM, vessels, OCS facilities and facilities currently subject to 33 C.F.R. part 104 – 106 would be required to implement a cybersecurity plan, principally based on CISA's cross-sector Cybersecurity Performance Goals. The cybersecurity plan is intended to "help detect, respond to and recover from cybersecurity risks that may cause transportation security incidents (TSIs)." The proposed rule imposes various cybersecurity requirements covering account security, device security, data security, personnel training, risk management (including cybersecurity assessments, penetration testing and routine system management), supply chain management, resilience, network segmentation, reporting and physical security. Additionally, covered entities would be required to establish a cybersecurity plan that "incorporates detailed preparation, prevention and response activities for cybersecurity threats and vulnerabilities." The proposed regulations identify specific sections that must be included within cybersecurity plans, including personnel training, cybersecurity systems and equipment, access controls, physical security controls, security incident reporting and cybersecurity assessments. If adopted as proposed, such cybersecurity plans must be submitted with a certification of compliance to the Coast Guard, which would be charged with approval of the plans submitted.

The maritime industry is encouraged to submit comments to this proposed rule no later than April 22, 2024. Specifically, the Coast Guard is seeking comments on whether it should (1) limit reporting requirements to only particular types of cyber incidents, (2) prescribe alternative methods to report incidents and (3) add cyber incident to the definition of hazardous condition. As all vessels, facilities and OCS facilities would be required to implement and abide by the cybersecurity measures, implement the mandated cybersecurity plan, and report suspicious activities, security incidents and data breaches, stakeholders should consider providing the Coast Guard with any comments, concerns or recommendations. Given the significance of the proposed regulations and the highly technical nature of the subject matter, the proposed cybersecurity regulations should generate robust comments.

Critical Port Infrastructure and Cybersecurtiy Considerations

Concurrent with the executive order, the White House also committed to investing US$20 billion over the next five years in port infrastructure through the president's Investing in America Agenda. Part of this investment is devoted to rebuilding the US' capacity to manufacture port cranes. The investment was prompted by concerns that Chinese cranes, which are essential to the loading, unloading and movement of containers at ports, pose a national security threat.

According to the White House, 80% of ship-to-shore cranes at US ports are manufactured in the People's Republic of China (PRC). The executive order states that PRC-made cranes represent a national security risk, as they have the potential to provide information to the PRC regarding US shipments, or to be remotely controlled to disrupt US supply chain operations.

The investment in US capabilities to manufacture cranes is part of broader efforts by the US government to protect US critical infrastructure from exploitation by nation-state actors, particularly by the PRC. These efforts include collaboration with the private sector and Department of Homeland Security (DHS) for alerts, warnings and threat hunting operations to identify malicious cyber activity.

Commercial Collaboration and Impacts

The heightened focus on PRC involvement in critical infrastructure has very recently impacted commercial decision-making. For example, the White House announced that PACECO Corp., a US subsidiary of Mitsui E&S Co., Ltd, intends to resume manufacturing cranes in the US. It will partner with other manufacturing companies to restore its US manufacturing capabilities after 30 years abroad. The US$20 billion investment will likely incentivize other manufacturers to onshore their operations, as well.

DHS's Role in Improving Supply Chain Resilience and Cybersecurity in the Maritime Industry

DHS also issued a fact sheet outlining its efforts to strengthen the cybersecurity of maritime critical infrastructure, including issuing a Maritime Security Directive[4] to take "immediate steps" to address and mitigate cyber-risk posed by PRC ship-to-shore cranes. Owners and operators of cranes must implement various measures with respect to PRC cranes and associated systems.

Furthermore, the DHS Supply Chain Resilience Center recently conducted a tabletop exercise among DHS stakeholders to test its response to cyberattacks on SRS cranes. The center will continue its efforts to address supply chain risk at US ports, as well as partner with the Department of Commerce to strengthen semiconductor supply chain, further the implementation of CHIPS and Science Act and develop supply chain early warning systems.

The Focus on China's Role in US Supply Chain

The measures outlined above highlight the focus of the administration's supply chain policy in protecting and mitigating against vulnerabilities inherent in dependence on China. US national security policy has and will continue to become increasingly intertwined with US economic regulation. For example, in addition to the maritime cybersecurity measures above, the National Defense Authorization Act (NDAA) for fiscal year 2024 prohibits federal funding for ports utilizing the PRC-sponsored National Transportation Logistics Public Information Platform (LOGINK). Similarly, the House introduced a bill, entitled Ocean Shipping Reform Implementation Act of 2023, that includes a provision prohibiting US port authorities from utilizing LOGINK. These recent actions demonstrate the heightened focus by the US government on China's potential impact on supply chains, and its intention to continue utilizing various authorities to address the perceived PRC threat to US national security, including in the maritime sector.

Conclusion

The actions outlined above underscore the federal government's continued commitment to enhance the nation's critical infrastructure cybersecurity. As outlined in the National Cybersecurity Strategy published last year, the administration is pursuing a multipronged approach to critical infrastructure cybersecurity, including in the maritime sector, which presents a mix of economic and national security concerns. While the draft regulations are not finalized, maritime and port entities, as well as other critical infrastructure providers, would be well advised to begin to bolster their cybersecurity posture while the rules are under consideration. Though the draft rules are complex and may appear daunting at first glance, maritime and other critical infrastructure providers can begin by conducting routine cybersecurity assessments and penetration testing to identify any security control gaps or vulnerabilities in their operations. Once such an assessment is conducted, entities are well equipped to establish a prioritized remediation plan based upon the risk presented by the vulnerabilities or gaps identified. Maritime entities and other critical infrastructure providers may also consider beginning to put together their cybersecurity plan now. Such a plan can help to outline and focus an organization's approach to cybersecurity. While the draft regulations may change, entities can likely assume that the contours of those regulations will remain. As technology rapidly advances, regulators and stakeholders will have to be prepared from a technological, commercial and legal perspective to meet the next generation of cyberthreats.

Contacts

Michael Kaye
Partner, Washington DC
T +1 202 457 6545
E michael.kaye@squirepb.com

Bridget McGovern
Partner, Washington DC
T +1 202 457 6104
E bridget.mcgovern@squirepb.com

Shea Leitch
Of Counsel, Washington DC
T +1 202 457 6510
E shea.leitch@squirepb.com

Darien Flowers
Principal, Washington DC
T +1 202 457 5336
E darien.flowers@squirepb.com

Sarah K. Rathke
Partner, Cleveland
T +1 216 479 8379
E sarah.rathke@squirepb.com

Michael J. Wray
Of Counsel, Houston
T +1 713 546 3330
E michael.wray@squirepb.com

John P. Flynn
Principal, Washington DC
T +1 202 457 5141
E john.flynn@squirepb.com

Michelle Story
Associate, Washington DC
T +1 202 457 5546
E michelle.story@squirepb.com

4 Although the Coast Guard announced MARSEC Directive 105–4 in the Federal Register, due to security concerns the text of MARSEC Directive 105–489 is not publicly available. Fed. Reg. 13726 (February 24, 2022)