BLANKROME

Maritime

FEBRUARY 3, 2025

Cybersecurity in the Marine Transportation System: What You Need to Know About the Coast Guard's Final Rule

The U.S. Coast Guard ("USCG") published a final rule on January 17, 2025, addressing Cybersecurity in the Marine Transportation System (the "Final Rule"), which seeks to minimize cybersecurity related transportation security incidents ("TSIs") within the maritime transportation system ("MTS") by establishing requirements to enhance the detection, response, and recovery from cybersecurity risks. Effective July 16, 2025, the Final Rule will apply to U.S.-flagged vessels, as well as Outer Continental Shelf and onshore facilities subject to the Maritime Transportation Security Act of 2002 ("MTSA"). The USCG is also seeking comments on a potential two-to-five-year delay of implementation for U.S.-flagged vessels. Comments are due March 18, 2025.

BACKGROUND

The need for enhanced cybersecurity protocols within the MTS has long been recognized. MTSA laid the groundwork for addressing various security threats in 2002 and provided the USCG with broad authority to take action and set requirements to prevent TSIs. MTSA was amended in 2018 to make clear that cybersecurity related risks that may cause TSIs fall squarely within MTSA and USCG authority.

Over the years, the USCG, as well as the International Maritime Organization, have dedicated resources and published guidelines related to addressing the growing cybersecurity threats arising as technology is integrated more and more into all aspects of the MTS. The USCG expanded its efforts to address cybersecurity threats throughout the MTS in its latest rulemaking, publishing the original Notice of Proposed Rulemaking ("NPRM") on February 22, 2024. The NPRM received significant public feedback, leading to the development of the Final Rule.

FINAL RULE

In its Final Rule, the USCG addresses the many comments received on the NPRM and sets forth minimum cybersecurity requirements for U.S.-flagged vessels and applicable facilities.

Training. Within six months of the Final Rule's effective date, training must be conducted on recognition and detection of cybersecurity threats and all types of cyber incidents, techniques used to circumvent cyber security measures, and reporting procedures, among others. Key personnel are required to complete more in-depth training.

Assessment and Plans. The Final Rule requires owners and operators of U.S.-flagged vessels and applicable facilities to conduct a Cybersecurity Assessment, develop a Cybersecurity Plan and Cyber Incident Response Plan, and appoint a Cybersecurity Officer that meets specified requirements within 24 months of the effective date.

There are a host of requirements for the Cybersecurity Plan, including, among others: provisions for account security, device protection, data safeguarding, training, drills and exercises, risk management practices, strategies for mitigating supply chain risks, penetration testing, resilience planning, network segmentation, reporting protocols, and physical security measures. Additionally, the Cyber Incident Response Plan must provide instructions for responding to cyber incidents and delineate the key roles, responsibilities, and decision-making authorities among staff.

Plan Approval and Audits. The Final Rule requires Cybersecurity Plans be submitted to the USCG for review and approval within 24 months of the effective date of the Final Rule, unless a waiver or equivalence is granted. The Rule also gives the USCG the power to perform inspections and audits to verify the implementation of the Cybersecurity Plan.

Reporting. The Final Rule requires reporting of "reportable cyber incidents"[1] to the National Response Center without delay. The reporting requirement is effective immediately on July 16, 2025. Further, the Final Rule revises the definition of "hazardous condition" to expressly include cyber incidents.

Potential Waivers. The Final Rule allows for limited waivers or equivalence determinations. A waiver may be granted if the owner or operator demonstrates that the cybersecurity requirements are unnecessary given the specific nature or operating conditions. An equivalence determination may be granted if the owner or operator demonstrates that the U.S.-flagged vessel or facility complies with international conventions or standards that provide an equivalent level of security. Each waiver or equivalence request will be evaluated on a case-by-case basis.

Potential Delay in Implementation. Due to a number of comments received related to the ability of U.S.-flagged vessels to meet the implementation schedule, the Final Rule seeks comments on whether a delay of an additional two to five years is appropriate.

CONCLUSION

As automation and digitalization continue to advance within the maritime sector, it is imperative to develop cyber security strategies tailored to specific management and operational needs of each company, facility, and vessel. Owners and operators of U.S.-flagged vessels and MTSA facilities are advised to review the new regulations closely and begin preparations for the new cybersecurity requirements at the earliest opportunity. Stakeholders are also encouraged to provide comments before March 18, 2025, addressing the potential two-to-five-year delay in implementation for U.S.-flagged vessels.

For more information and assistance, contact Dana S. Merkel, Vanessa C. DiDomenico, Holli B. Packer, or another member of Blank Rome's Maritime group.

Dana S. Merkel
202.772.5973 | dana.merkel@blankrome.com

Vanessa C. DiDomenico
617.415.1176| vanessa.didomenico@blankrome.com

Holli B. Packer
215.569.5488 | holli.packer@blankrome.com

1. A reportable cyber incident is defined as an incident that leads to, or, if still under investigation, can reasonably lead to any of the following: (1) substantial loss of confidentiality, integrity, or availability of a covered information system, network, or operational technology system; (2) disruption or significant adverse impact on the reporting entity's ability to engage in business operations or deliver goods or services, including those that have a potential for significant impact on public health or safety or may cause serious injury or death; (3) disclosure or unauthorized access directly or indirectly of non-public personal information of a significant number of individuals; (4) other potential operational disruption to critical infrastructure systems or assets; or (5) incidents that otherwise may lead to a TSI as defined in 33 C.F.R. 101.105.