U.S. Coast Guard Cybersecurity Rule 2025

Cybersecurity Readiness at Sea

Introduction

On July 16, 2025, the U.S. Coast Guard's (USCG) Final Rule on Cybersecurity (the "Final Rule") enters into force, further acknowledging the growing importance of managing cyber risk in a shipping industry that has long been cyber immature but increasingly digitized, automated and integrated. This marks another key evolutionary step in promulgating a maritime cybersecurity compliance regime. While primarily intended to strengthen domestic maritime infrastructure under the Maritime Transportation Security Act ("MTSA"), its presumptive reach extends well beyond U.S. flagged vessels and domestic terminals. To this end, the Final Rule sends a strong signal to non-U.S. flagged commercial vessels calling on US ports that cyber risk management is now a key focus for the U.S. Government in general and the USCG's Port State Control program specifically.

While the Final Rule primarily targets U.S. vessel operators with clearly defined timelines out to 2027, it indirectly affects foreign flagged vessels calling on U.S. ports, which may need to adapt their cybersecurity practices to ensure compliance alignment with the cybersecurity standards of their U.S. partners and peers.

The Final Rule specifically amends 33 Code of Federal Regulations and while not legally binding on foreign flagged ships outside U.S. waters, any vessel subject to USCG Port State Control (PSC) inspections will be expected to demonstrate adherence to the cybersecurity best practices that should already be present in the vessel's Safety Management System ("SMS"). This represents *de minimis* risk, and going forward shipowners will be well served to implement a cyber risk posture consistent with the Final Rule's standards. As there are already inconsistencies among PSC inspections on the subject of cybersecurity, shipowners should take action to ensure that their vessels can operate without delay, scrutiny, or liability within U.S. waters.

Core Components of the Final Rule and Implications for Shipowners

The USCG's Final Rule does not introduce new regulations *per se* but formally integrates cyber risk management best practices into the MTSA's existing regulatory framework. Key requirements include but are not limited to:

- Mandatory cybersecurity assessments within Vessel Security Plans.
- Appointment of a *Cybersecurity Officer* (CySO) to oversee cyber risk mitigation.
- Reporting of cyber incidents to the National Response Center within 12 hours.
- Required training in cyber threat detection and response, aligned with physical security.
- Enforcement measures such as denial of entry or delay of operations for non-compliance.

Cyber threats are real and with threat actor adoption of Artificial Intelligence (AI) increasingly sophisticated, customized and effected at scale. Recognizing this, the USCG has drawn a line in the sand and failure to adhere to cybersecurity best practices may result in enforcement actions that include denial of entry, delayed cargo operations, or the imposition of control measures. Vessels arriving at a U.S. port without demonstrable cyber risk management best practices in place elevate the risk to the health, safety and security of the maritime transportation system and the environment, which may result in operational disruption, environmental harm, injury or death, liability exposure, reputational damage, and financial loss. Even more, USCG investigations now include a cyber component and USCG Cyber Protection Teams have been deployed to support such investigations through analysis and evidence collection.

Key Considerations for Shipowners

Although the Final Rule's effects on foreign flagged vessels may be nuanced as of this publication, its impact is not insubstantial. To mitigate the potential for operational disruption and actively demonstrate a proactive commitment to USCG defined cybersecurity standards, non-U.S. shipping companies would be wise to proactively align their policies with the Rule.

Here are a few key considerations:

- **Heightened USCG expectations:** Failure to demonstrate cyber readiness may result in delayed entry, inspection holds, or penalties. Examples of such failures include evidence of poor cyber hygiene (e.g. hand-written passwords), the absence of cybersecurity assessments or crew unfamiliarity with cyber incident response and reporting protocols.
    - ***Recommendation:*** *Review all training materials for cybersecurity awareness for seafarers and officers. Update content to reflect cybersecurity threat identification, incident reporting and response. Complete training by January 12, 2026.*

- **Unharmonized standards:** The Final Rule emphasizes cybersecurity assessments to inform the Ship Security Plan (SSP). However, the ISM and ISPS Code do not emphasize cyber risk factors to the Rule's extent. USCG Port State Control Officers (PSCOs) will likely analyze the SSP for cybersecurity updates and whether cyber risk factors have been incorporated into contingency planning and/or procedures.
    - ***Recommendation:*** *Review and update SSPs to align with IMO MSC-FAL.1/Circ.3/Rev.3* – Guidelines on Maritime Cyber Risk Management *(Section 3.5) and cross-matrix against Final Rule expectations. Be sure to emphasize alignment with cyber incident reporting, response and recovery capabilities.*

- **Conduct a Cybersecurity Gap Assessment:** Review current Ship Security Plan (SSP) against the Rule's requirements and identify cybersecurity capability gaps (e.g., people, processes, procedures, controls, tools).
    - **Recommendation:** It is strongly recommended to conduct a comprehensive cybersecurity gap assessment onboard each vessel to evaluate the extent to which current Ship Security Plans align with the Rule. This assessment should actively evaluate vulnerabilities across both Information Technology (IT) and Operational Technology (OT) environments and identify and address any deficiencies related to the Rule, including the integration of cyber risk into existing security frameworks. Additionally, to ensure harmonization, cross-map Rule elements with MSC-FAL.1/Circ.3/Rev.3.

- **Review and Update Ship Security Plans (SSPs) – Recommended Guidance:** Integrate cyber threats into SSPs in accordance with IMO MSC-FAL.1/Circ.3 and align with U.S. MTSA standards where possible. This will serve as vessel's evidence of preparedness. Reflect cyber threats, access controls, business continuity measures and digital forensics response in the SSP. Identify physical security controls for IT and OT systems.

- **Draft a Cybersecurity Plan – Recommended Guidance for US Flagged Vessels:** Harmonize it with cybersecurity components in the SMS, SSP and Contingency Plans. Where appropriate, cross-map these to IACS UR E26 and E27 standards. Cybersecurity Plan elements should include or cross-reference to:
    - CySO identification (and associated authorities)
    - Training, drills and exercises
    - Documentation and recordkeeping
    - Communications
    - Cybersecurity measures for monitoring and maintenance of critical systems
    - Recordkeeping; inspections, audits and plan amendments
    - Incident reporting, response and recovery

  Key cybersecurity measures should include:
    - Account Security Measures for IT/OT systems (e.g., minimum password strengths, multi-factor authentication, the principle of least privilege and other credential management protocols)
    - Data Security Measures (e.g., logging is performed and log data protected, encryption is employed to ensure the integrity of IT and OT traffic).
    - Device security measures (e.g., approved asset inventory, application controls, network inventory and mapping).
    - Segmentation of IT and OT networks
    - Performance of vulnerability scans (as per the Cybersecurity Plan)
    - Regular risk assessments of critical IT and OT assets and systems
    - Security Patch Management / Configuration Management integrated with Management of Change processes
    - Cybersecurity criteria for IT and OT vendors
    - Remote access and monitoring oversight and controls
    - Regular Backups of critical IT and OT systems

- **Develop Cyber Incident Response Protocols:** Establish clear procedures for cyber incident identification, escalation and alert criteria; protocols for reporting cyber events, including escalation timelines and contact points such as the National Response Center.
    - **Recommendation:** Identify cybersecurity response capabilities, reporting and engagement criteria for the Qualified Individual (see also below). Specifically:
        - Draft (or update existing) a Cyber Incident Response (IR) Plan.

- Document U.S. specific contact information and procedures for NRC reporting within the Cyber IR Plan
- Ensure cybersecurity best practices and procedures are tested and understood across the crew (especially those identified in the SMS).

- **Identify a Cybersecurity Officer (CySO):** While the Rule requires all US regulated entities to designate a Cybersecurity Officer (CySO), a formal position responsible for implementing cybersecurity policies and ensuring compliance with the Rule, this does not apply (yet) to foreign vessels. The CySo must ensure the appropriate personnel implement the Cybersecurity and Cyber IR Plans. The CySO must also ensure that the Cybersecurity Plan is up to date and undergoes an annual audit, arrange for cybersecurity inspections, ensure that personnel have adequate cybersecurity training, record and report cybersecurity incidents to the owner or operator and take steps to mitigate them.
    - ***Recommendation:*** *Identify a CySO as soon as feasible. Doing so will align with PSCO inspections and facilitate cyber incident reporting, response and recovery communications. Doing so also aligns with the governance recommendations in MSC-FAL.1/Circ.3/Rev.3. While the Ship's Master can serve as CySO, consider assigning this responsibility to another officer (e.g., Chief Mate, Chief Engineer). This will allow the Master to remain focused on overall vessel operations during emergencies where seaworthiness may be impacted. Identify the CySO in the Cyber IR Plan.*

- **Ensure Appropriate Incident Reporting is in Place:** This obligation applies equally to all U.S. and foreign flagged vessels. The Rule requires that all cyber incidents be reported to the U.S. National Response Center (NRC) within 12 hours. If a cyber incident compromises a vessel's seaworthiness or undermines the vessel's ability to comply with U.S. port security regulations, reporting is mandatory, regardless of flag state. Examples of such events include GPS spoofing, unauthorized access to OT and/or IT systems, denial of service attacks against navigational systems and/or malware impacting critical systems.
    - ***Recommendation:*** *Ensure the designated CySO is aware of the 12-hour reporting window and the shipboard procedures guiding this activity. In the event a CySO has not been identified, ensure the vessel's Master and Ship Security Officers are aware. Consider also incorporating this into a quarterly drill or annual exercise consistent with the ISPS Code requirements. Ensure the Cyber IR Plan identifies all required reporting protocols for reporting to the NRC.*

- **Review and Update Crew Awareness / Training:** Cybersecurity training is expected to be completed by January 12, 2026, and USCG PSCOs will be incorporating cybersecurity into their inspections. Increased scrutiny will occur and crew familiarity will be expected for enhanced cyber threat recognition; access controls for Information Technology (IT) and Operational Technology (OT) systems; incident response, recovery and reporting; and contingency procedures in the event of a disruptive attack.

- *__Recommendation:__ Design cybersecurity drills that are realistic and incorporate cyber event scenarios into existing ISPS drills. Also incorporate cybersecurity measures into existing ISPS drills and training programs. Ensure training content aligns with U.S. expectations on awareness, response and communications.*

Re-Think the Role of the Qualified Individual in Enhancing Cyber Resilience

To support alignment with the Final Rule and strengthen its cybersecurity response posture, we encourage shipping companies to identify and contract with a Qualified Individual (QI) with demonstrated expertise in maritime cybersecurity. The QI's cybersecurity liaison will serve as the primary advisor and coordinator for all cyber risk management activities, including but not limited to:

- Overseeing the integration of cybersecurity into SSPs.
- Drafting supplemental cybersecurity guidance for a shipping company's technical and procedural safeguards for IT and OT systems.
- Identify the QI in the Cyber IR Plan.
- Leading cybersecurity incident response coordination
- Liaising with US port authorities, US Federal State and Local regulatory agencies, law enforcement (e.g., FBI, state and local authorities), where applicable, and emergency responders and USCG Captain of the Port designated Cyber Liaison Officers.
- Collaborate and coordinate with USCG Cyber Protection Teams.
- Leading incident response coordination with specialty Digital Forensics and Incident Response (DFIR) organizations.
- Advising on compliance with evolving cybersecurity requirements under MTSA, IMO and flag state regimes.
- Conducting regular cybersecurity training and tabletop exercises to maintain operational readiness across shipboard and shoreside personnel.

By embedding cybersecurity capabilities within the QI role, non-US flagged shipping companies ensure that cyber risk management is proactive—promoting early threat detection, rapid incident response and continuous improvement. This alignment of operational security and cybersecurity within a single, accountable role provides a critical resilience advantage in an increasingly complex threat environment.

Conclusion: Cyber Compliance as a Condition of Market Access

Although the USCG's Final Rule is fundamentally a US requirement it establishes new cybersecurity standards and benchmarks for cyber resilience in the maritime transportation system; it also elevates expectations. For non-U.S. flagged commercial vessels, the potential costs of implementing *de minimis* cybersecurity capabilities or inaction heightens the risk of detentions, delays, reputational harm and lost revenue and/or fines. The chronic challenge of cybersecurity regulations in any form is that they have been established often in reaction to changing threats and as a result are always in catch up mode in the face of today's cyber threat landscape. As a result, any minimalist cybersecurity posture focused entirely on compliance is in itself inherently vulnerable and costly in the long term.

The USCG's Final Rule broadens the cybersecurity baseline and while non-U.S. flagged vessels may not be legally obligated to the Final Rule's provisions the practical consequence of ignoring it undeniable. Disruptive cyber incidents are impacting all areas of the maritime transportation system. Establishing a proactive cyber compliance program should now factor in the compliance posture of all ships entering US waters.

Intentional alignment with the Final Rule will position the fleet vis-à-vis the USCG as a trusted trading partner in an increasingly risky cyber threat environment. Shipowners investing early in aligning their organization's cybersecurity capabilities and best practices will not only reduce the potential for regulatory friction but also cultivate a competitive advantage in a market increasingly targeted by threat actors and shaped by operational cyber resilience (or cyber immaturity). Expanding the operational cybersecurity program to the Final Rule's cybersecurity performance objectives should be thought of as a strategic imperative that reduces financial, liability and operational risk. This approach changes the question from an optional *should we comply* to *how we will comply* and that's good business for everyone.

Acknowledgement:

This publication was written in collaboration with ShorelineHudson (Acrisure), an international provider of business risk solutions supporting the maritime transportation system, as well as the government, insurance and energy sectors. Their insights and expertise contributed significantly to the content of this publication.

About the Authors

Max Bobys is a recognized leader in maritime cybersecurity, currently serving as Vice President and Practice Director of Cyber Risk Management at ShorelineHudson, a leading global maritime risk management firm. In this role, he oversees all aspects of client delivery, including cybersecurity strategy and advisory, enterprise risk management, governance, risk, compliance, board advisory, tailored threat intelligence, and training services. With over 20 years of experience in enterprise risk management and transformation, Mr. Bobys is recognized for his expertise in designing and implementing integrated cyber-physical/security systems. Specifically, he led the team that developed and now delivers Hudson's award-winning (2017 Lloyds List Winner for Digital Innovation) *CyberLogix* application suite to ports, terminal operators, and some of the world's largest global shipping companies. His cybersecurity advisory experience also extends to airport authorities, gas utilities, and manufacturing. Committed to advancing cybersecurity best practices and fostering collaboration within the industry, Mr. Bobys regularly presents at international conferences, facilitates executive workshops, and publishes articles and white papers on maritime cybersecurity with an eye to demystifying the complexities of cybersecurity to enable informed decision-making.

Lauren Wilgus is the Director of Steamship Mutual Insurance Services North America, LLC based in the United States. Prior to joining the Club, Lauren was a Partner in the New York Maritime Litigation Group of an Am Law 100 law firm, where she spent over 16 years handling a wide range of complex maritime matters. Her experience includes both wet and dry shipping disputes, maritime attachment and vessel arrest actions, judgment recognition and enforcement proceedings, and regulatory matters before the Federal Maritime Commission.

Taslim Imad is a Loss Prevention Manager with more than 32 years of experience in the shipping industry. He holds an MBA in Shipping and Logistics and is a qualified Master Mariner, having served at sea on various types of vessels. Since coming ashore in 2012, he has worked for a major PCTC operator. Before joining Steamship Mutual P&I Club, he was employed by a respected and whitelist Flag Administration. Taslim is well-versed in IMO conventions and international regulations. Drawing on both his seafaring and shore-based experience, he understands the perspectives of all stakeholders in the industry. He now represents the Club at various seminars and committees, focusing on safety and risk management issues.