U.S. Coast Guard Cybersecurity Rule 2025
Key Legal Issues, Deadlines and FAQS

On January 17, 2025, the U.S. Coast Guard published a final rule establishing comprehensive cybersecurity requirements for the Marine Transportation System (MTS). This rule, effective July 16, 2025, is designed to minimize cybersecurity related transportation security incidents (TSIs) and protect critical maritime infrastructure from evolving digital threats. For owners and operators of U.S. flagged vessels, onshore facilities, and Outer Continental Shelf (OCS) facilities, understanding the legal implications and compliance deadlines is essential.

Scope and Applicability of the Rule

The new U.S. Coast Guard Cybersecurity Rule (Rule) applies to a broad range of entities within the maritime sector. Specifically, it covers owners and operators of U.S. flagged vessels, facilities, and OCS facilities that are required to maintain a security plan. Notably, foreign flagged vessels are excluded from these requirements. The rule is designed to address the unique cybersecurity risks present in the maritime environment, where Operational Technology (OT) and Information Technology (IT) systems are increasingly interconnected and vulnerable to cyber threats. The U.S. Coast Guard's authority to regulate cybersecurity in this context stems from the Maritime Transportation Security Act of 2002 (MTSA), which was amended in 2018 to explicitly include cybersecurity risks.

Compliance Requirements and Timelines

The Rule sets forth a series of phased compliance deadlines and following requirements.

- The rule takes effect on July 16, 2025, requiring all "reportable cyber incidents" to be reported to the National Response Center (NRC).
- By January 12, 2026, all personnel must complete cybersecurity training.
- Additionally, key personnel are required to undergo in-depth training on their roles and responsibilities during a cyber incident, as well as how to stay current with evolving threats and countermeasures.
- Training for new hires, or those gaining access to new IT or OT systems, must also be completed within five days of system access, but no later than 30 days after hiring, and must be repeated annually.
- Within 24 months of the rule's effective date, by July 16, 2027, owners and operators must conduct a comprehensive Cybersecurity Assessment, develop and submit a Cybersecurity Plan and a Cyber Incident Response Plan for U.S. Coast Guard approval and designate a qualified Cybersecurity Officer (CySO).

Ongoing Obligations: Drills, Exercises, and Audits

After the U.S. Coast Guard approves the Cybersecurity Plan, owners and operators are required to conduct cybersecurity drills at least twice per calendar year and cybersecurity exercises at least once per calendar year, with no more than 18 months between exercises. The cybersecurity portion of the plan and the results of penetration tests must be made available to the U.S. Coast Guard upon

request. The U.S. Coast Guard also retains the authority to conduct inspections and audits to verify compliance and the effectiveness of implemented cybersecurity measures.

Waivers, Equivalency, and Potential Delays

Recognizing the diversity of operations and the potential challenges of implementation, the rule allows for limited waivers or equivalency determinations. A waiver may be granted if an owner or operator can demonstrate that the cybersecurity requirements are unnecessary due to the specific nature or operating conditions of their vessel or facility. Alternatively, an equivalency determination may be granted if the entity can show compliance with international conventions or standards that provide an equivalent level of security. Each request is evaluated on a case-by-case basis, providing some flexibility for unique operational circumstances.

Conclusion: Proactive Steps for Compliance

As the industry adapts to this new regulatory environment, it is critical for owners and operators to stay informed and proactive. By taking early and comprehensive action, maritime stakeholders can not only achieve compliance but also strengthen their overall cybersecurity posture, reducing the risk of costly incidents and enhancing resilience in an increasingly digital world.

FAQ: 2025 U.S. Coast Guard Cybersecurity Rule

What is the purpose of the new U.S. Coast Guard cybersecurity rule?

The rule aims to minimize cybersecurity-related Transportation Security Incidents (TSIs) within the Marine Transportation System (MTS) by establishing baseline requirements for detecting, responding to and recovering from cybersecurity risks. It is designed to address the growing threat landscape as maritime operations become more automated and digitally interconnected.

Who Does the New U.S. Coast Guard Cybersecurity Rule Apply to?

Under the U.S. Coast Guard C.F.R requirements, the new cyber security regulations apply to:

1. U.S. flagged vessels required to have a security plan under 33 C.F.R. § 104;
2. Facilities required to have a security plan under 33 C.F.R. § 105, and;
3. Outer Continental Shelf facilities required to have a security plan under 33 C.F.R. § 106.

When does the rule take effect and what are the key compliance deadlines?

- ***Effective Date***: July 16, 2025.

- ***Immediate Reporting***: As of July 16, 2025, all reportable cyber incidents must be reported to the National Response Center (NRC).

- ***Training Deadline***: By January 12, 2026, all personnel must complete required cybersecurity training.

- ***Assessment and Plan Submission***: By July 16, 2027, owners and operators must conduct a Cybersecurity Assessment, develop and submit a Cybersecurity Plan and Cyber Incident Response Plan to the Captain of the Port (COTP), and designate a Cybersecurity Officer (CySO).

What constitutes a "reportable cyber incident" and to whom do I report it?

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 nonpublic 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.

Further, the Final Rule revises the definition of "hazardous condition" to expressly include cyber incidents. Incidents must be reported to the National Response Center (NRC).

What is the job of the Cybersecurity Officer?

Each covered entity must designate a Cybersecurity Officer (CySO) responsible for implementing and maintaining cybersecurity requirements. The rule allows for designation of alternate CySOs and permits one individual to serve multiple vessels or facilities.

What are the training requirements under the rule?

All personnel must be trained to recognize and detect cybersecurity threats and incidents, understand techniques used to circumvent cybersecurity measures, and know how to report incidents. Those working with operational technology (OT) require OT specific training. Key personnel must receive additional, in-depth training on their roles during a cyber incident and how to stay current with evolving threats. Training for new hires or those accessing new IT/OT systems must be completed within five days of system access, but no later than 30 days after hiring, and must be repeated annually.

What are the ongoing obligations after the Cybersecurity Plan and Cyber Incident Response Plan has been approved?

Owners and operators must conduct cybersecurity drills at least twice per calendar year and cybersecurity exercises at least once per calendar year, with no more than 18 months between exercises. The cybersecurity portion of the plan and penetration test results must be available to the Coast Guard upon request. The Coast Guard may also conduct inspections and audits to verify compliance.

Are there any provisions for waivers or equivalency?

Yes. Owners and operators may request a waiver if they can demonstrate that the cybersecurity requirements are unnecessary due to their specific operations. Alternatively, an equivalency determination may be granted if the entity complies with international conventions or standards that provide an equivalent level of security. Each request is evaluated individually.

Acknowledgement:

This publication was written in collaboration with BLANKROME LLP, a top law firm based in the United States known for their practice in maritime law, advising global shipping clients on regulatory compliance, vessel finance, sanctions, litigation, and environmental enforcement.

About the Authors

Dana S. Merkel is a partner in the Maritime Practice Group at Blank Rome LLP, based in the firm's Washington, D.C. office. Dana focuses her practice on domestic and international marine transportation and environmental issues for clients worldwide. She provides compliance counseling under a myriad of international conventions and U.S. and foreign regulations, assists clients in enforcement actions, and provides support following marine casualties. Dana also conducts customized training sessions for clients and assists in creating and implementing effective compliance programs. In 2025, Dana was listed as "Next Generation Partner" in The Legal 500's Guide to Up-and-Coming Lawyers Nationwide.

Holli B. Packer is an associate in the Maritime Practice Group at Blank Rome LLP, based in the firm's Philadelphia Office. Holli's practice spans a broad spectrum of maritime and environmental issues, from maritime casualties, Jones Act personal injury, and pollution incidents to federal and state enforcement actions, regulatory compliance, and crisis response. She assists vessel owners/operators, charterers, and waterfront facilities on regulatory compliance related to the IMO, U.S. Coast Guard, U.S. EPA, U.S. Customs and Border Protection, and other federal and state agencies. In 2025, Holli was named one of the Top 40 Young Lawyers "On the Rise" by the American Bar Association.

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.