Marine Safety Information Bulletin

Commandant
U.S. Coast Guard
Inspections and Compliance Directorate
2703 Martin Luther King Jr Ave, SE, STOP 7501
Washington, D.C. 20593-7501

MSIB Number: MSIB 04-26
Date: August 19, 2026
E-Mail: MTSCyberRule@uscg.mil

Applicability of MTSA Cybersecurity Requirements to Inactive Vessels

The Coast Guard is issuing this bulletin to clarify that MTSA cybersecurity requirements continue to apply to vessels that are "Inactive" but retain a valid Certificate of Inspection (COI) or Certificate of Compliance (COC). This bulletin also clarifies the distinction between "Laid Up" and "Inactive" vessel status during nonoperational periods. Under *CVC-WI-018(3)*, a vessel is considered "Laid Up" only when the Certificate of Inspection (COI) or Certificate of Compliance (COC) has been formally surrendered with a request to the cognizant Officer in Charge, Marine Inspection (OCMI) for removal from service. Vessels placed in "Laid Up" status are not required to comply with 33 CFR Subchapter H requirements. Conversely, vessels retaining a valid COI but otherwise "Inactive" (for reasons such as operational seasonality, drydock, or extended dockside maintenance) must continue to comply with applicable parts in 33 CFR Subchapter H and their approved Vessel Security Plan (VSP) or Alternative Security Program (ASP).

Cybersecurity risks remain present year-round. Even when secured for maintenance or seasonality, vessel networks, operational technology, remote access pathways, and vendor interfaces (including portable media) remain vulnerable to compromise. Periods of inactivity can elevate risk due to reduced manning, deferred updates, unattended systems, and third-party maintenance. Operators are responsible for maintaining existing security measures, ensuring that third-party and vendor access to Information Technology (IT) and Operational Technology (OT) systems is strictly controlled, monitored, and documented.

MTSA cybersecurity regulations in *33 CFR Part 101 Subpart F* mandate cybersecurity training for all personnel, including temporary and permanent contractors, accessing U.S.-flagged vessel or facility IT and/or OT systems. While general training requirements took effect January 12, 2026, specific Cybersecurity Plan (CSP) training may be deferred until CSP approval or July 16, 2027, whichever is earlier. Operators are responsible for controlling third-party access. Section 13 of CG-5PC Policy Letter 01-25 outlines compliance pathways for contractor training.

For further information, please email the Coast Guard's Office of Maritime Cybersecurity Policy (CG-MCP) at MTSCyberRule@uscg.mil or visit the Coast Guard Maritime Cybersecurity Resource Center.

-uscg-