The U.S. Coast Guard Cybersecurity Regulations for the Marine Transportation System

Small Entity Compliance Guide for MTSA-regulated Facilities and OCS Facilities

Docket: To view documents mentioned in the final rule as being available in the docket, go to *www.regulations.gov*, type USCG-2022-0802 in the search box, and click "Search." Next, in the Document Type column, select "Supporting & Related Material."

For further information about this document, email MTSCyberRule@uscg.mil or call Commander Brandon Link, Office of Port and Facility Compliance at 202-372-1107.

For additional cybersecurity resources visit the Coast Guard Maritime Industry Resource Center at https://www.uscg.mil/MaritimeCyber/.

The Basics of the Rule

The Coast Guard is updating its maritime security regulations by establishing minimum cybersecurity requirements for U.S.-flagged vessels, Outer Continental Shelf (OCS) facilities, and facilities subject to the Maritime Transportation Security Act of 2002 (MTSA) regulations. This final rule addresses current and emerging cybersecurity threats in the marine transportation system by adding minimum cybersecurity requirements to help detect risks and respond to and recover from cybersecurity incidents. These include requirements to develop and maintain a Cybersecurity Plan, designate a Cybersecurity Officer (CySO), and take various measures to maintain cybersecurity within the marine transportation system.

We formulated minimum cybersecurity requirements that may assist firms and regulated entities with their cybersecurity posture in an effort to reduce the likelihood, vulnerability, and risk of a cyber incident. If a cyber incident occurs, the Coast Guard believes that these minimum cybersecurity requirements will mitigate its impact on firms, regulated entities, and the U.S. economy, and create the intended benefits for regulated entities.

The Components of Cybersecurity in the Marine Transportation System

33 CFR Subchapter F

101.600 Purpose.
101.605 Applicability.
101.610 Federalism.
101.615 Definitions.
101.620 Owner or operator.
101.625 Cybersecurity Officer.
101.630 Cybersecurity Plan.
101.635 Drills and exercises.
101.640 Records and documentation.
101.645 Communications.
101.650 Cybersecurity measures.
101.655 Cybersecurity compliance dates.
101.660 Cybersecurity compliance documentation.
101.665 Noncompliance, waivers, and equivalents.
101.670 Severability.

Frequently Asked Questions

Am I covered by this final rule?

You are covered by this final rule if you are an owner or operator of a facility or an OCS facility required to have a security plan under title 33, Code of Federal Regulations (CFR), parts 105 and 106.

What are my cyber incident reporting responsibilities as a small entity?

This final rule did not create new **cyber incident** reporting requirements for MTSA-regulated facilities that are subject to **33 CFR 6.16-1**; however, it did add a definition for "**reportable cyber incident**" and created a requirement for **entities that have not reported to the Coast Guard pursuant to, or are not subject to, 33 CFR 6.16-1,** to report all **reportable cyber incidents** to the National Response Center (NRC) per § 101.620(b)(7). 33 CFR 6.16-1 does not apply to OCS facilities regulated under 33 CFR part 106. Therefore, MTSA-regulated OCS facilities are subject to the reporting requirements in 33 CFR 101.620.

Background on "cyber incident" and "reportable cyber incident" reporting requirements:

On February 21, 2024, Executive Order 14116 on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States amended 33 CFR part 6. Among other provisions, it added a definition for "**cyber incident**" and created a requirement to report evidence of an actual or threatened cyber incident involving or endangering **any vessel, harbor, port, or waterfront facility** to the Coast Guard, the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA). The broad

applicability of 33 CFR part 6 and the new definition of a cyber incident created an overlap with existing MTSA reporting requirements.

Cyber incident means an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system, or actually jeopardizes, without lawful authority, an information system.

On January 17, 2025, the Coast Guard updated its maritime security regulations by establishing minimum cybersecurity requirements for U.S.-flagged vessels, facilities, and OCS facilities subject to MTSA regulations. Among other provisions, it added a definition for "**reportable cyber incident**" and created a requirement for **entities that have not reported to the Coast Guard pursuant to, or are not subject to, 33 CFR 6.16-1,** to report all reportable cyber incidents to the NRC per § 101.620(b)(7).

Reportable cyber incident means an incident that leads to or, if still under investigation, could reasonably lead to any of the following: (1) Substantial loss of confidentiality, integrity, or availability of a covered information system, network, or OT 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 transportation security incident as defined in 33 CFR 101.105.

Are there waivers or equivalents to this final rule for small entities?

Yes, per § 101.665, an owner or operator, **after completing the required Cybersecurity Assessment**, may seek a waiver or an equivalence determination for the requirements in subpart F consistent with the waiver and equivalence provisions in 33 CFR 105.130, 105.135, 106.125, and 106.130.

§ 105.130 Waivers.
Any facility owner or operator may apply for a waiver of any requirement of this part that the facility owner or operator considers unnecessary in light of the nature or operating conditions of the facility, prior to operating. A request for a waiver must be submitted in writing with justification to the Commandant (CG-5P), Attn: Assistant Commandant for Prevention Policy, U.S. Coast Guard Stop 7501, 2703 Martin Luther King Jr. Avenue SE., Washington, DC 20593-7501. The Commandant (CG-5P) may require the facility owner or operator to provide data for use in determining the validity of the requested waiver. The Commandant (CG-5P) may grant, in writing, a waiver with or without conditions only if the waiver will not reduce the overall security of the facility, its employees, visiting vessels, or ports.

§ 106.125 Waivers.
Any OCS facility owner or operator may apply for a waiver of any requirement of this part that the OCS facility owner or operator considers unnecessary in light of the nature or operating conditions of the OCS facility. A request for a waiver must be submitted in writing with justification to the cognizant District Commander. The cognizant District Commander may require the OCS facility

owner or operator to provide additional data for use in determining the validity of the requested waiver. The cognizant District Commander may grant a waiver, in writing, with or without conditions only if the waiver will not reduce the overall security of the OCS facility, its personnel, or visiting vessels.

What are the requirements for the waiver submissions for small entities?

- Waivers should be submitted on signed formal correspondence and include:
    - Copy of the Cybersecurity Assessment.
    - Specific requirement(s) requested to be waived.
    - Justification for why a requirement is not applicable or why a facility or an OCS facility is unable to comply with the specific requirement(s).

§ 105.135 Equivalents.
For any measure required by this part, the facility owner or operator may propose an equivalent as provided in § 101.130.

§ 106.130 Equivalents.
For any measure required by this part, the OCS facility owner or operator may propose an equivalent, as provided in § 101.130.

What are the requirements for equivalence submissions for small entities?

- Requests for approval of equivalent cybersecurity measures should be submitted on signed formal correspondence and include:
    - Specific requirement(s) requested for equivalency.
    - Justification of the proposed equivalency.
    - Comparison on how the alternative complies with the intent of a requirement in question.

Additionally, as noted in § 101.660, the Alternative Security Program (ASP) provisions apply to cybersecurity compliance documentation and are addressed in 33 CFR 105.140 for facilities, and 33 CFR 106.135 for OCS facilities. Given the unique nature of cybersecurity threats, vulnerabilities, and mitigation strategies, owners and operators must ensure that use of ASPs includes those items specific to each facility and OCS facility. The Coast Guard will evaluate each ASP's cybersecurity component to ensure full regulatory compliance with each applicable requirement. The owners and operators will not be required to submit separate Plans to the Coast Guard and will be able to include a Cybersecurity Plan as part of an approved ASP.

To further reduce the burden for impacted entities, the Coast Guard has extended the compliance deadline for the required Cybersecurity Assessment from 12 months to 24 months, and the compliance deadline for the Cybersecurity Plan from after the second annual audit of the existing physical security plan to 24 months.

Does the Coast Guard provide credit, equivalence, or exemption to owners and operators of small entities who already have similar structures in place to comply with these regulations?

The Coast Guard does not provide a blanket credit, equivalence, or exemption based on a regulated entity's compliance with similar regulations or requirements. An owner or operator of a facility or an OCS facility may use those structures to inform their Cybersecurity Assessment, Cybersecurity Plan, and compliance with this final rule and, as needed, may follow the procedures in § 101.665 to request a waiver or equivalence determination.

When compliance with similar or parallel regulations or requirements is the basis for an owner or operator to request a waiver, the Coast Guard notes that the owner or operator must still detail the portions of the Coast Guard's regulation they meet, and the specific measures taken under that similar or parallel compliance when requesting a waiver or equivalency. An owner or operator simply stating that they are complying with equivalent measures does not provide the Coast Guard with enough information to ensure regulatory compliance.

What are the responsibilities of owners and operators of small entities if some systems on board the facility are fully managed by the system vendor?

Owners and operators are ultimately responsible for the systems and equipment at their facility or OCS facility. They should work with vendors to identify what security measures are in place that could meet the requirements of these regulations, or how they will adjust to ensure systems and equipment are secured.

What types of grants are available for small entities?

The Coast Guard will seek to work with the Federal Emergency Management Agency (FEMA) to further highlight cybersecurity through the FEMA-administered Port Security Grant Program. Because we do not manage that program, we cannot make any representation about future prioritization of grant funds. As noted in FEMA's Fiscal Year 2024 Notice of Funding Opportunity for this program, all entities subject to an Area Maritime Transportation Security Plan, as defined by 46 U.S.C. 70103(b), may apply for program funding.[1] Eligible applicants include but are not limited to port authorities, facility operators, and State, local, and territorial government agencies. FEMA identified enhancing cybersecurity as a key priority for Fiscal Year 2024. Please visit https://www.fema.gov/grants/preparedness/port-security for additional information.

What is the timing of this final rule's requirements?

This final rule is effective July 16, 2025.

Immediately upon the effective date of this final rule:

- Entities that have not reported to the Coast Guard pursuant to, or are not subject to, 33 CFR 6.16-1 begin ensuring that all reportable cyber incidents are reported to the NRC per § 101.620(b)(7).

[1] See FEMA, "The U.S. Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2024 Port Security Grant Program," April 16, 2024, https://www.fema.gov/print/pdf/node/676012, accessed October 23, 2024.

Within 6 months from the effective date of this final rule and annually thereafter:

- All personnel must complete the training specified in § 101.650(d)(1)(ii) through (v) that includes recognition and detection of cybersecurity threats and all types of cyber incidents, techniques used to circumvent cybersecurity measures, procedures for reporting a cyber incident to the CySO, and operational technology (OT)-specific cybersecurity training (for all personnel whose duties include using OT).
- Key personnel (for example, personnel with access to information technology (IT) or remotely accessible OT systems, including contractors, whether part-time, full-time, temporary, or permanent) must also complete the training specified in § 101.650(d)(2) about their roles and responsibilities during a cyber incident and response procedure and how to maintain current knowledge of changing cybersecurity threats and countermeasures.

Within 24 months from the effective date of this final rule:

- Owners and operators must designate, in writing, the CySO per § 101.620(b)(3) and (c)(1).
- Owners and operators must submit the Cybersecurity Plan to the Coast Guard for approval within 24 months of the effective date of this final rule per § 101.655.
- Owners and operators must conduct the Cybersecurity Assessment within 24 months of the effective date of this final rule and annually thereafter (or sooner than annually if there is a change in ownership) per § 101.650(e)(1).

After receiving approval of the Cybersecurity Plan:

- Owners and operators must conduct cybersecurity drills at least twice each calendar year.
- Owners and operators must also conduct cybersecurity exercises at least once each calendar year with no more than 18 months between cybersecurity exercises per § 101.635(b)(1) and (c)(1).
- Each owner or operator must ensure that the cybersecurity portion of their Plan and penetration test results are available to the Coast Guard upon request per § 101.660.
- All personnel must complete the training specified in § 101.650(d)(1)(i) within 60 days of receiving approval of the Cybersecurity Plan.

We want to assist small entities in understanding this final rule so they can better evaluate its effects on them. If this final rule affects your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please email MTSCyberRule@uscg.mil or call Commander Brandon Link, Office of Port and Facility Compliance at 202-372-1107.