USCG Office of Cybersecurity Policy (CG-MCP) Mission Management System (MMS) Work Instruction (WI)

Category	Administrative				
Title	Waiver and Equivalency Guidance for Requirements of 33 CFR Part 101, Subpart F - Cybersecurity				
Serial	MCP-WI-002	Orig. Date	03June26	Rev. Date	N/A
Signature Authority	C. N. Parham Chief, Office of Maritime Cybersecurity Policy				
Disclaimer:	This guidance is not intended to, nor does it, impose legally binding requirements on any party. The regulatory requirements in reference (a) remain in effect and are unchanged by this policy letter. It is advisory in nature and intended to ensure consistent application of 33 CFR Part 101, Subpart F provisions across all regulated entities. The guidance represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the public, and the Coast Guard, as well as other federal and state regulators, in applying statutory and regulatory requirements.				
References:	a) Title 33, Code of Federal Regulations (CFR), Part 101.665 b) CG-5PC Policy Letter 01-26, Cybersecurity Assessment: Initial Scoping and Process				
Enclosures:	(1) Decision Guidance for Waivers and Equivalencies under 33 CFR 101.665 (2) Recommended Process for Submitting a Waiver or Equivalency Request Waiver Application Process (3) Submission Checklist (4) Waiver Request Letter Template Upon Determination of No/Minimal Risk				

A. Purpose. This work instruction provides guidance for waivers and equivalency determinations of cybersecurity requirements under 33 CFR 101, Subpart F - Cybersecurity, as provided in reference (a).

B. Action. The Coast Guard and industry should use this work instruction for the submission, approval, and maintenance of waivers and equivalencies for cybersecurity requirements as allowed by reference (a). This guidance harmonizes guidance for vessels, facilities, and Outer Continental Shelf (OCS) facilities for the preparation and submission of requests for a cybersecurity requirement to be waived or satisfied through an equivalent measure that achieves the same or higher level of protection.

C. Background. The regulations in 33 CFR Part 101, Subpart F – Cybersecurity became effective on July 16, 2025. This subpart sets minimum cybersecurity requirements for U.S.-flagged vessels, facilities, and OCS facilities to safeguard the security and resilience of the Marine Transportation System (MTS). Per reference (a), an owner or operator, after completion of the required Cybersecurity Assessment (CSA), may seek a waiver or an equivalency determination for the requirements in 33 CFR Part 101, Subpart F using the standards and submission procedures applicable to a U.S.-flagged vessel, facility, or OCS facility as outlined in 33 CFR 101.130, 104.130, 104.135, 105.130, 105.135, 106.125, or 106.130. The CSA forms the evidentiary basis for waiver and equivalency determinations.

D. Applicability. This work instruction applies to all U.S.-flagged vessels, facilities, and OCS facilities required to have a security plan under 33 CFR 104, 105, and 106. In this guidance, MTSA-regulated vessels, facilities, and OCS facilities will be referred to collectively as "entities" for brevity; however, it does not change the specific responsibility designations in Reference (a). If this guidance is intended to apply to a

particular subset of entities, it will be specifically identified. This work instruction will be distributed by electronic means only. It is available at the USCG Maritime Industry Cybersecurity Resource Website.

E. Policy.

1. A waiver is a formal request by an owner or operator, submitted after completing the Cybersecurity Assessment (CSA), as required by Reference (a), asking the Coast Guard to grant relief from a specific cybersecurity requirement in 33 CFR 101 Subpart F that the owner or operator considers unnecessary in light of the nature or operating conditions of the entity.

2. An equivalency is a formal request by an owner or operator, submitted after completing the CSA, as required by Reference (a), asking the Coast Guard to use alternative safeguard(s) that meet or exceed the effectiveness as a requirement in the regulation.

   The following enclosures are provided to assist owners/operators with the submission of waiver and/or equivalency requests:

   a. Enclosure (1): Guidance - deciding whether to request a waiver or equivalency.
   b. Enclosure (2): Guidance - recommended process to prepare and submit a request.
   c. Enclosure (3): Checklist - as a guide to help ensure complete submission.
   d. Enclosure (4): Template - no/minimal IT/OT waiver request.

F. Consistency and Transparency. A unified process ensures that all MTS entities, regardless of size, type, or digital maturity, follow the same sequence for waiver and equivalency determinations. By basing every request on a completed CSA as outlined in Reference (b), the Coast Guard can maintain national consistency in evaluation of requests while preserving flexibility for unique operational conditions.

G. Enclosures.

1. Enclosure (1) to CG-MCP-WI-002.pdf
2. Enclosure (2) to CG-MCP-WI-002.pdf
3. Enclosure (3) to CG-MCP-WI-002.pdf
4. Enclosure (4) to CG-MCP-WI-002.pdf

C.N. Parham

C. N. PARHAM
Chief
U.S. Coast Guard Office of Maritime
Cybersecurity Policy
By direction

Enclosure (1)
Decision Guidance for Waivers and Equivalencies under 33 CFR 101.665

This document provides USCG personnel with information to help address common questions that MTSA-regulated vessel, facility, and OCS facility owner/operators may pose as it relates to requests for a waiver or equivalency under 33 CFR 101.665. It is provided in Question-and-Answer format for clarity and ease of use.

Section 1 — General Questions

1. **What is a waiver?**
   A waiver is a formal request by an owner or operator, submitted after completing the Cybersecurity Assessment (CSA), asking the Coast Guard to grant relief from specific cybersecurity requirement(s) in 33 CFR 101 Subpart F that the owner or operator considers unnecessary in light of the nature or operating conditions of the entity.

2. **What is an equivalency?**
   An equivalency is a formal request by an owner or operator, submitted after completing the CSA, asking the Coast Guard to use alternative safeguard(s) or process(es) that meet or exceed the effectiveness as a requirement in the regulation. It allows an operator to comply with the intent of the requirement through a different, but equally effective, method.

3. **33 CFR 101.665 also mentions temporary deviations and requesting permission to operate. What are the differences and similarities between waivers, equivalencies and temporary deviations?**

	Waiver	Equivalency	Temporary Deviation
Purpose	Used when the owner or operator (O/O) requests relief from a regulatory requirement.	Used when the O/O can achieve the requirement's intent via another means.	Used when the O/O reports they cannot comply with a requirement for a short period of time, but requests permission to continue operations in the interim.
Requirement	The requirement is excused.	The requirement still applies.	The requirement applies but cannot be met temporarily.
Owner/Operator Request	O/O considers the requirement unnecessary in light of the nature or operating conditions.	O/O proposes an alternative method, program, or standard to meet the requirement.	O/O demonstrates that a short-term condition prevents full compliance.
Objective	Recognize that the requirement cannot or does not need to be met.	Meet or exceed the same level of security as the requirement.	Manage security risk during a temporary loss of compliance.

Lifespan	Long-term regulatory relief.	Permanent or long-term compliance solution.	Strictly short-term and must be corrected.

SECTION 2 — Waivers

4. **Can I request a waiver before completing the CSA?**
   No. The regulation makes clear that the CSA must be completed first, even if the assessment identifies that there is no IT or OT systems or equipment to assess. The request must be supported by the CSA and demonstrate that granting the waiver will not reduce the entity's overall security or increase risk of a Transportation Security Incident. For specific submission requirements, see checklist in Enclosure (3).

5. **When may I request a waiver?**
   An owner/operator may request a waiver any time after completing a CSA.

6. **What criteria should I consider when requesting a waiver?**
   Ultimately, the owner/operator is permitted to apply for a waiver of any requirement in 33 CFR 101 Subpart F that the owner/operator considers unnecessary in light of the nature or operating conditions of the entity. Reviewing the following criteria may help in deciding whether to request a waiver:

   a. The system or capability exists in your operational environment.
   b. The requirement clearly applies to that system.
   c. You are unable to meet the requirement due to technical, architectural, or operational constraints.
   d. The CSA demonstrated that leaving the vulnerability/risk that a requirement addresses unprotected will not materially impact the safety, security, or operations of your entity or the MTS.

7. **Should I request a waiver "just in case" to avoid noncompliance?**
   No. Waivers should not be used as a protective measure against uncertainty.

8. **Should I request a waiver for 33 CFR 101.650(a), (b), or (c) requirements that apply only to networks, systems, or devices that I do not have in my environment?**
   No. Waivers are not necessary for a requirement that does not apply under 33 CFR 101.650. A waiver provides a path for relief from a requirement that applies to the entity. Conversely, a waiver is not applicable for a system, feature, or capability that is not installed within the environment. This should be identified in the CSA and documented in the CSP with an explanation of non-applicability. To ensure clarity during inspections and audits, owners and operators should note that the requirement was evaluated.

   > **Example**: 33 CFR 101.650(a)(4) requires multi-factor authentication (MFA) for remotely accessible operational technology (OT). If a vessel's architecture does not include remote OT access, the MFA requirement is not waived; it is correctly designated as "Not Applicable" (N/A) with written explanation in the CSP.

*Relief from requirements in any situation or paragraph other than that which is addressed in Question #8 must be proposed in a waiver request. If in doubt as to whether Question #8 applies to your situation, contact the Coast Guard for guidance.

9. **Can I use a waiver request to tell the Coast Guard what sections I will comply with instead?**
   No. Waiver requests identify the specific regulatory citations from which relief is requested and provide justification for the request, while maintaining compliance with all other regulatory provisions. Requests that are submitted stating the regulatory sections that will be complied with, rather than requests for waiver of specific regulatory section(s) will be returned for revision. The Coast Guard will evaluate whether the requirements of the regulations may be waived and not materially impact the entity's operations, safety, and/or security.

10. **Can I request a waiver for hypothetical future systems or configurations?**
    No. The Coast Guard cannot grant pre-emptive waivers for hypothetical future architectures or technologies. Waivers must be based on actual, current system configurations, or specific, detailed plans for new systems/devices/processes with predicted timelines for completion, which, if the waiver is approved, will be installed/modified by the owner or operator as presented in the request.

11. **Can I request a waiver for an entire section of the regulation?**
    Yes. Particularly for entities with entirely manual operations, or those who have already received a waiver from 33 CFR 104, 105, or 106, a waiver from 33 CFR 101 Subpart F may be appropriate depending on the outcome of the CSA. Each requested waiver must be justified based on CSA evidence and risk analysis. If granted, the Coast Guard may retain certain requirements necessary for maritime coordination, operations, safety, and security.

12. **Can I base a waiver request solely on cost, staffing, or convenience?**
    No. Cost, staffing, and convenience may provide relevant context but are not sufficient justifications on their own. Waivers must address the risk accepted if the waiver is granted and be grounded in technical, architectural, or operational constraints that prevent compliance as written.

13. **Can vendor preference or reluctance be the basis for a waiver?**

    No. Vendor convenience or reluctance is not by itself a valid justification. If a vendor product cannot be replaced and truly cannot support required safeguards, the CSA and waiver request must describe the technical limitations, the associated risks, and the lack of feasible compensating controls or alternative means of compliance. If compensating controls or alternative means are available, consider an equivalency instead of a waiver.

SECTION 3 — Equivalency

14. **Can I request an equivalency before completing the CSA?**

No. The regulations in 33 CFR 101.665 and preamble to the Final Rule make clear that the CSA must be completed first, even if the assessment identifies that there is no IT or OT systems or equipment to assess. The request must be supported by the CSA and demonstrate that granting the equivalency will not reduce the entity's overall security or increase risk of a Transportation Security Incident.

15. When should an owner/operator request an equivalency?

An equivalency is appropriate when:

a. The requirement applies to the entity, and
b. You cannot meet the requirement exactly as written, but
c. You can achieve the requirement's intent via another means.

16. When are compensating security controls considered acceptable to "meet the requirement" and when are they an "alternate means to meet the requirements intent," requiring an equivalency request?

a. Compensating controls are considered acceptable without an equivalency request when:
   i. Specifically allowed in regulation (for example, in 33 CFR 101.650(a)(2)); or,
   ii. When used to address a vulnerability that does not correlate with a specific regulatory requirements.
b. Compensating controls are alternate means to meet the requirement's intent, requiring an equivalency request when the regulations state a specific control or action and do not specify allowance for compensating controls.

17. Can an owner or operator submit an equivalency request based on compliance with a classification society standard or an industry cybersecurity framework?

Yes. Owners and operators may base an equivalency request on their compliance with a recognized classification society standard or industry cybersecurity framework. The Coast Guard will consider these requests when the submitted information clearly shows that the portions of the standard relied upon meet or exceed the intent of the applicable requirements in 33 CFR Part 101, Subpart F.

To support this type of request, you should provide:

a. A crosswalk that identifies how the specific sections of the standard you are relying on meet or exceed the *specific regulatory requirements* included in your equivalency request.
b. Proof of current, valid certification under the standard, or documentation demonstrating compliance with the relevant portions of the standard when the standard does not include a formal certification program.

18. What if my vendor cannot modify their product to meet a cybersecurity requirement that applies to that function on my network?

a. Document it by describing the vendor restriction and its impact in your Cybersecurity Assessment and Cybersecurity Plan.

b. You may check alternatives by asking the vendor for any built-in controls or compensating measures they support, or consider alternate vendors that do meet the requirement.
c. If compliance with the requirement is still impossible as written, submit a waiver or equivalency request under 33 CFR 101.665 based on the documented limitation and CSA risk evaluation.
d. Temporary need: If this creates an immediate compliance gap, notify the COTP/MSC and request temporary deviation while the waiver is processed.

Enclosure (2)

Recommended Process for Submitting a Waiver or Equivalency Request Waiver Application

Step	Action	Details
1. Conduct Cybersecurity Assessment	Before applying for a waiver of any provision(s) of 33 CFR 101 Subpart F, the owner or operator must complete the required Cybersecurity Assessment.	This is a prerequisite for seeking a waiver, as the assessment provides the necessary context and data to justify why a particular requirement might be unnecessary.
2. Prepare the Waiver Request	The owner or operator must prepare a formal written request.	The request must be submitted as signed formal correspondence. It should include the items listed in the applicable checklist of Enclosure (3).
3. Submit the Request	The waiver request is submitted to the appropriate Coast Guard authority.	For facilities and vessels, the request is submitted to the Commandant (CG-5P). For Outer Continental Shelf (OCS) facilities, the request goes to the cognizant District Commander.
4. Coast Guard Review	The Coast Guard will review the waiver request.	The Coast Guard may require the owner or operator to provide additional data to support the request. The review will assess whether the proposed waiver would reduce the overall security of the vessel or facility.
5. Decision	The Coast Guard will issue a written decision.	A waiver may be granted, with or without conditions, or denied.

Equivalency Application Process

Step	Action	Details
1. Identify the Alternative	The owner or operator identifies or develops an alternative security measure, system, or procedure.	The regulation allows for equivalents, as the Coast Guard recognizes that technology and security practices evolve.
2. Develop the Justification	Prepare a detailed analysis demonstrating the effectiveness of the proposed equivalency.	This is the most critical part. The request must not just describe the alternative; it should demonstrate its equivalence. This may involve a comparative security analysis, technical specifications, or operational data.
3. Prepare the Formal Request	The owner or operator must prepare a formal written request.	The request must be submitted as signed formal correspondence. It should include the items listed in the applicable checklist of Enclosure (3).
4. Submit the Request	The request is submitted to the appropriate Coast Guard authority.	For all entities, the request is submitted to the Commandant (CG-5P).
5. Coast Guard Review	The Coast Guard evaluates the proposed equivalency request.	The Coast Guard may require the owner or operator to provide additional data to support the request. The review will assess whether the proposed equivalence meets or exceeds the effectiveness of the regulatory requirement.
6. Decision	The Coast Guard will issue a written decision.	If the Coast Guard is satisfied with the proposed measures, the equivalency will be approved, which is then implemented in place of the standard requirement. If not, the owner/operator will be notified in writing of the decision.

Enclosure (3)

Submission Checklist

Submission Checklist

This checklist is provided as the best practice guide to help ensure your submission is complete, aligned with 33 CFR 101.665, and ready for review. If the entity has minimal to no IT or OT, refer to enclosure (4) to determine whether applying for a waiver under that option would be more appropriate.

For All Requests:

☐ Identify specific entity(ies), including Official ID or Number (One entity per request. In the case of a single CSP for multiple similar entities, one CSP per request)

☐ Provide point of contact for request

☐ Attach Cybersecurity Assessment (CSA) report for each entity, completed and current; see Reference (b) for guidance

☐ Identify specific regulatory requirement(s) (cite the CFR section(s)) for which waiver or equivalency is sought (one or multiple requirements may be included in one request))

☐ Ensure applicability of regulatory requirement(s) confirmed in the CSA

☐ Define the scope of the request (system, condition, or requirement) and whether any critical IT/OT is involved

---

For Vessels:

☐ A copy of the Certificate of Inspection (COI)

☐ A list of other Captain of the Port Zones this vessel operates in, if any

☐ Operational details including typical cargoes carried, waterways typically transited, and whether the vessel has interconnectivity with any facilities

☐ State if the systems/devices/processes involved in the request are or are not connected to or reliant upon external network(s) (provide detail if ‘yes’) or if they are they locally hosted, operated, or isolated

☐ Do you provide a unique or critical service as part of the MTS (e.g. sole provider of transportation to remote area, sole source/one of few sources of supply of entity product(s), significant market share of product to region/area)

☐ If other vessels under the same owner/operator have made or will make a similar request, list the vessels and their official numbers (O.N.)

For Facilities:

☐ List the facility name, ID, and cognizant COTP Zone

☐ Facility type and profile of facility operations - including products, worst case discharge (if applicable), passenger throughput (if applicable),

☐ Interconnectivity to pipelines/rail/intermodal/other facilities and/or interconnectivity with any vessels

☐ Is there shared infrastructure or dependency on/of the involved network/system/devices/processes by any other entities or companies, such as in a landlord port or the requesting entity as a service delivery provider.

☐ Any connectivity to or reliance on corporate network or are subject systems/devices/processes locally hosted/operated

☐ Do you provide a unique or critical service as part of the MTS (e.g. sole provider of transportation to remote area, sole source/one of few sources of supply of entity product(s), significant market share of product to region/area)

Additional Items — Equivalency

☐ Description of existing and/or proposed alternate safeguards or controls

☐ Detailed explanation of how the existing and/or proposed alternate safeguards or controls meets or exceeds the effectiveness of the regulatory requirement

☐ Any other technical, procedural, governance, or other information pertinent to the request to describe management of cybersecurity risk

---

Additional Items — Waiver

☐ Explanation of (1) why the requirement is unnecessary or (2) why the entity cannot comply with it - be specific as to why the requirement is unnecessary in light of the nature or operating conditions of the entity. Describe any inherent technical, architectural, or operational constraints. In evaluating why the requirement may or may not be necessary, considerations include, but are not limited to:

☐ Would the requested waived requirement impact critical IT/OT if implemented? Would implementing the requirement reduce the risk of (1) a TSI or (2) Cyber Incident (as defined/harmonized in NVIC 02-24 (series))? What would be the operational impact if system/device/process/function were disrupted because the requirement was not implemented?

☐ Does the requirement impact or replace a system/device/process/function that is a human safety barrier or is it related to/would it impact an automated safety system (prevent loss of life, injury, or harm to environment)?
☐ Would the requirement reduce the risk of a cascading impact across interconnected systems if implemented? Would the requirement affect system/device/process/ functions that are integrated with/dependent on other systems? Would the requirement only impact air-gapped systems/devices and if so, has airgap been recently validated?
☐ Any other pertinent information to justify request

Final Quality Check

Before submitting, ask:

☐ Is this request specific, not broad or speculative?
☐ Would an independent reviewer be able to understand the request without guessing intent?

Enclosure (4)

Waiver Request Letter Template Upon Determination of No/Minimal Risk

Company Letterhead Month Day, Year

Commandant (CG-MCP)
2703 Martin Luther King Jr Avenue SE
Washington DC 20593

Subject: Waiver Request from Title 33, Code of Federal Regulations, Part 101 Subpart F

Dear Sir/Ma'am,

I am writing as the owner/operator or authorized representative of the owner/operator of <entity name>. The legal owner/operator company is <company name, address>. My facility/vessel is subject to 33 CFR 104/105 . I understand that I am currently subject to 33 CFR 101 Subpart F, Cybersecurity; however, I believe that my facility/vessel should receive a full waiver from these requirements.

(if facility) <Entity name> is located at <address> in Captain of the Port <name> Zone. Description: *description of operations should include a detailed explanation of operations within the entire facility footprint, any applied reduction in MTSA footprint through NVIC 03-03(series), the nature of the facility's operations in the area (e.g. vital or sole source supplier of <commodity> for area, utility serving ___ households, etc.)*

(if vessel) <Entity name> is a <type of vessel> and the Certificate of Inspection is attached. Description: *include a copy of the current Certificate of Inspection (COI), a digital photo of your vessel; a description of typical cargoes carried, operating areas, and routes; the nature of the vessel's operations (e.g., single ferry operation to island, regular supplier to isolated location; support of national defense, etc.)*

(*If applicable)* I currently have reduced/no MTSA compliance requirements because I received a partial or full waiver from 104/105 on date. I have attached the waiver letter to this request.

The owner/operator has assessed the infrastructure and operations and:

a. There is minimal/no IT and minimal/no OT as defined in 33 CFR 101.615. If minimal, the IT and/or OT consists of the systems and devices listed in the table below (fill in each column with the system and specific device name, function, interconnectivity with any other device/system/internet, and its use in operations (if any), add additional rows if necessary.

IT/OT System List

System + Specific Device	**Function**	**Interconnectivity *(Yes/No)* *If Yes, describe***	**Used in Operations or Physical Security Functions*(Yes/No)* *If Yes, describe***

b. If minimal, the items listed above could not lead to any of the following:

1. A substantial loss of confidentiality, integrity, or availability of an information system, network, or OT system beyond the items listed in the table above;
2. Disruption or significant adverse impact on the entity's ability to engage in business operations or deliver goods or services;
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; and,
5. Incidents that may lead to a transportation security incident.

I request a waiver from all of the requirements of 33 CFR 101 Subpart F. I will maintain a point of contact for the Coast Guard at all times, which will be <name> who can be reached at <phone number> and <email>. I understand that:

a. If any of the attested to conditions above change, including the point of contact, I must notify the cognizant Captain of the Port (COTP) in a timely manner and I may be required to resubmit for a waiver or come into compliance with 33 CFR 101 Subpart F.

b. I am required to notify the Coast Guard of a cyber incident as outlined in NVIC 02-24 (series) and 33 CFR 6.16-1.

Certification and Attestation

Under penalty of law (18 U.S.C. § 1001), I declare that I am the authorized representative for the owner or operator listed above. I certify that the information provided in this document is true and accurate to the best of my knowledge and that the regulated facility/vessel meets the assertions outlined above.

Printed Name:
Title:
Signature:
Date:

Instructions:

1. *Use of this template letter is not required. It is provided as guidance, however the Coast Guard encourages entities to use this template as it identifies the relevant information that will aid the evaluation of the waiver request. If this template, or a substantially similar letter, is used, it is recommended to complete all sections that are applicable to your operation (facility/vessel). Remove sections indicated for non-applicable operations. Ensure all mentioned documents are included with your request. Add any additional information that you believe may be pertinent to the adjudicator of the waiver request.*

2. *This template waiver request is intended for entities that have minimal to no IT or OT within the full scope of the entity's operation and that the IT or OT could not cause a cyber incident as defined in the harmonized definition in NVIC 02-24 (series). As a general matter, entities that are typically eligible for this waiver use fully manual processes in operations. Any technology is minimal and not relied upon for safe and secure operations. Example entities with minimal IT or OT include, but are not limited to:*

    a. *A vessel or facility with a single OT monitoring system that has human/manual backup or is not relied upon for safety/security;*
    b. *A small facility with a small number of computers located in a main office used for basic administrative tasks. Computers do not store personal information and the tasks could easily be done manually, absorbed by another branch/office, or would not significantly disrupt business if compromised.*

3. *Submission using this streamlined template is not a guarantee of waiver approval. Your request may be deemed inadequate and the request returned for revision and resubmission.*

4. *Entities with IT or OT that could lead to a cyber incident or TSI and that desire a waiver of any provision of 33 CFR 101 Subpart F should not use this template and must complete a full cybersecurity assessment and request a waiver with justification for each provision under 33 CFR 101.665.*

5. *Submit the signed form to the Office of Maritime Cyber Policy (CG-MCP).*

6. *Retain a copy of this completed request as a record with your Facility Security Plan (FSP) or Vessel Security Plan (VSP).*