

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26



Commandant
United States Coast Guard

2703 Martin Luther King Jr. Ave. SE
Washington DC 20593-7318
Staff Symbol: CG-5P

NVIC 02-26
October 19, 2026

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26

Subj: CYBERSECURITY REGULATIONS IMPLEMENTATION GUIDANCE FOR
MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATED ENTITIES

Ref: (a) Title 33, Code of Federal Regulations (CFR), Part 101 Subpart F
(b) 46 United States Code (USC) § 70103(c)(3)(A)
(c) Title 33, Code of Federal Regulations, Part 6
(d) USCG Office of Maritime Cyber Policy (CG-MCP) Mission Management System (MMS) Work Instruction MCP-WI-002, Waiver and Equivalency Guidance for Requirements of 33 CFR Part 101, Subpart F - Cybersecurity
(e) National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, published February 26, 2024
(f) NIST Special Publication (SP) 800-53, Revision 5
(g) Navigation and Vessel Inspection Circular (NVIC) No. 02-24 (series)
(h) Laid-up Inspected/Examined Vessels, CVC-WI-018(3)
(i) CG-MCP MMS Work Instruction MCP-WI-003, DoD SAFE Instructions for Cybersecurity Plan, Cybersecurity Assessment, Waiver & Equivalency Request Submissions

1. PURPOSE. This NVIC provides information and guidance on the implementation of cybersecurity regulations for MTSA-regulated entities. These regulations were published in the Federal Register on January 17, 2025 (90 FR 6298) and are available in Title 33, Code of Federal Regulations, Part 101 (33 CFR 101). This NVIC is also intended to clarify the regulatory text, aid the cyber risk management process for the maritime industry, and present the Coast Guard's preferred means of complying with the subject regulations.

2. DISCLAIMER.

- a. This NVIC is intended only to provide clarity regarding existing requirements under the law. It does not change any legal requirements and does not impose new requirements on the public. Not all recommendations will apply to all entities, depending on individual operations, systems, equipment, or other factors. The Coast Guard recognizes that the entities comprising the Marine Transportation System (MTS) are varied in cybersecurity resources, programs, and overall/specific risks. Owners/operators may use a different approach that has greater or lesser complexity than this NVIC recommends, if that approach satisfies the applicable legal requirements. Entities are strongly encouraged to utilize best practices and industry standards, such as the NIST Cybersecurity Framework, and to mature their cybersecurity programs in a timely fashion to address evolving threats, vulnerabilities, and associated risks.

- b. Throughout this NVIC, “must”, “should”, and “may” are used purposefully. While the regulations set minimum requirements and are generally referenced by “must,” the guidance in “should” and “may” statements highlight recommended practices that are consistent with global cybersecurity standards.
3. TIMELINE. On January 17, 2025, the Coast Guard updated its maritime security regulations by establishing minimum cybersecurity requirements for U.S.-flagged vessels, facilities, and Outer Continental Shelf (OCS) facilities required to have a security plan under 33 CFR Parts 104, 105, and 106. The cybersecurity regulations came into effect on July 16, 2025, and are available in 33 CFR 101 Subpart F. MTSA regulated entities are required to operate in accordance with this regulation and their submitted Cybersecurity Plan (CSP) as of July 16, 2027.
4. DIRECTIVES AFFECTED.
 - a. NVIC 01-20, Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities, is cancelled, as it is superseded by this guidance reflecting updated cybersecurity requirements under 33 CFR Part 101, Subpart F.
 - b. CG-5PC Policy Letter 01-25, Cybersecurity Training for Personnel with Access to Information Technology (IT) or Operational Technology (OT) Systems, dated October 9, 2025, remains in effect until July 16, 2027, at which point it will be cancelled as relevant contents are incorporated into Chapter 2.b of Enclosure (1) to this NVIC.
 - c. CG-5PC Policy Letter 01-26, Cybersecurity Assessment Initial Scoping and Process, dated June 2, 2026, is cancelled as contents are incorporated into Enclosure (4) of this NVIC.
5. DISCUSSION.
 - a. The Coast Guard’s oversight of cybersecurity within the MTS is rooted in performance-based evaluation, where inspectors confirm that entities have implemented security measures that reduce cyber risk and sustain operational resilience. The MTSA regulations remain focused on performance-based requirements, in which the expected standard of performance is set, and the exact method of compliance is left up to the owner/operator in consideration of varied business needs, operating environments, vulnerabilities, risk environment, and risk tolerance. For example, just as the original MTSA regulations do not specify that a facility must have a fence to achieve physical access control, the MTSA cybersecurity regulations do not require a specific method for conducting network credential management. Owner/operator intent alone is insufficient; performance can and should be validated through documentation and observable evidence of implementation, effectiveness, and risk management. This approach gives owners/operators the discretion to determine the internal details of how they will meet the regulatory standards in the most effective and efficient way for their organization. The Coast Guard will not specify any particular solutions or products to address the requirements. Restating the regulatory text in CSP sections can be helpful for organization and reference. However, because of the performance-based nature of many requirements, if this approach is used, owners/operators must ensure they are also documenting how they are specifically meeting each requirement in the CSP.

- b. In this NVIC, MTSA-regulated vessels, facilities, and OCS facilities will be referred to collectively as “entities” for brevity, and responsible parties will be collectively referred to as “owners/operators”; however, this does not change the specific responsibility designations in reference (a). If guidance is intended to apply to a particular subset of entities, it will be specifically identified. The Cybersecurity Plan developed under reference (a) will be referred to as “CSP.” The Cybersecurity Assessment will be referred to as “CSA.” Except where noted, this guidance will refer to the Vessel Security Plan (VSP), Facility Security Plan (FSP), and Outer Continental Shelf Facility Security Plan (OCS FSP) developed under 33 CFR 104, 105, or 106 collectively as “security plan.”
 - c. The CSP serves as the foundational framework for an entity’s cybersecurity program. For entities newly embarking on formalizing their cybersecurity efforts, the CSP establishes baseline governance to structure and define their program. For entities with a mature cybersecurity governance program that exceeds the standards set by these regulations, the CSP may be a regulatory compliance document that cross-references existing cybersecurity practices to MTSA requirements.
 - d. As the CSP is central to the compliance program and most security requirements in the regulations must be annotated within the CSP in some fashion, implementation guidance on various topics is organized according to the section of the CSP in which they would be included. This NVIC is a companion document to the regulations and is intended to augment rather than be used as a stand-alone compliance guide. Ultimately, owners/operators must ensure that all regulatory provisions are complied with in accordance with 33 CFR 101.620(a). Table 1 of Enclosure (1) provides a crosswalk of regulatory provisions to CSP sections to guide CSP development and ensure all regulatory provisions are covered in the CSP.
 - e. For clarity, implementation guidance is developed as if the required provisions of reference (a) are included in a CSP that is either a separate document or a standalone annex of the security plan. Owners/operators may include compliance information incorporated into the security plan as outlined in 33 CFR 101.630, and all provisions in this guidance still apply. While the CSP may be incorporated into an existing security plan, this does not mean that the CSP is expected to be less complex to develop or maintain than a separate document or an annex of the security plan. In general, the provisions outlined in these cybersecurity regulations are meant to reflect a similar depth and scope as the physical security provisions established by MTSA.
 - f. MTSA-regulated owners/operators are encouraged to use the guidance provided in Enclosures 1-4 to develop and maintain a robust and resilient cybersecurity posture for their operations, as well as in preparation for cybersecurity-focused compliance inspections by Coast Guard personnel. Enclosures to this NVIC include Cybersecurity Plan Development and Maintenance Guidance, a Sample Cybersecurity Officer (CySO) Designation Letter, Penetration Testing Guidance, and Scoping and Assessment Guidance.
6. ACTION. Captains of the Port (COTPs) and Officers in Charge, Marine Inspection (OCMIs) are encouraged to bring this circular to the attention of maritime entities within their zones of responsibility. This NVIC will be distributed by electronic means only. It is located on the

[Coast Guard's Navigation and Vessel Inspection Circular website](#) and can also be accessed via the [Coast Guard's Maritime Industry Cybersecurity Resource Center](#).

7. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. The Office of Environmental Management, Commandant (CG-SHORE-V) reviewed this NVIC and the general policies contained within and determined that this policy falls under DHS categorical exclusion A3. This NVIC will not result in any substantial change to existing environmental conditions or violation of any applicable federal, state, or local laws relating to the protection of the environment. It is the responsibility of the action proponent to evaluate all future specific actions resulting from this policy for compliance with the National Environmental Policy Act (NEPA), other applicable environmental requirements, and the U.S. Coast Guard Environmental Planning Policy, COMDTINST 5090.1 (series).
8. RECORDS MANAGEMENT CONSIDERATIONS. Records created as a result of this publication, regardless of format or media, must be managed in accordance with Records & Information Management Program Roles and Responsibilities, COMDTINST 5212.12 (series) and the records retention schedule location on the Records Resource Center Microsoft SharePoint site.
9. FORMS/REPORTS. None. The U.S. Coast Guard handles all Sensitive Security Information (SSI), in accordance with 49 CFR 1520, which includes requirements for proper information marking and storage. The information is therefore not subject to routine public disclosure. The U.S. Coast Guard will share the information with other agencies on a need-to-know basis and in accordance with applicable laws and policies.
10. QUESTIONS. Questions concerning this policy should be directed to the U.S. Coast Guard Office of Maritime Cybersecurity Policy (CG-MCP) at MTSCyberRule@uscg.mil.



Robert C. Compher
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Prevention Policy

Enclosure: (1) Cybersecurity Plan Development and Maintenance Guidance
(2) Sample CySO Designation Letter
(3) Penetration Testing Guidance
(4) Scoping and Assessment Guidance

Enclosures

Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance	6
Enclosure (2) - Sample CySO Designation Letter	48
Enclosure (3) - Penetration Testing Guidance	52
Enclosure (4) - Scoping and Assessment Guidance.....	55

Tables

Table 1 - Regulatory provisions to CSP sections crosswalk.....	10
Table 2 - Example responsibility matrix for a landlord/tenant arrangement at a cruise terminal.	14
Table 3 - Personnel Training Requirements.....	23
Table 4 - Cybersecurity Drill and Exercise Requirements.....	25
Table 5 - Guidance for CSP Sections 7, 8, and 9	33
Table 6 - Compliance Purposes and Timelines.....	38
Table 7 - Compliance Event Scenarios	38
Table 8 - CSA Process Guide.....	58

Figures

Figure 1 - Compliance Flowchart	11
Figure 2 - Port with One FSP vs. Port with Individual FSPs	14
Figure 3 - Cyber Incident Response Lifecycle.....	44
Figure 4 - Categorization of Network Assets and Systems.....	56
Figure 5 - CSA Risk Filtering Process	57

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

Enclosure (1)

Cybersecurity Plan Development and Maintenance Guidance

Table of Contents

1. CYBERSECURITY PLAN – GENERAL	9
a. Organization.....	9
b. Notation.....	9
c. Alternate Section Format.	9
d. Development.	9
e. Scope.....	9
f. Governance.	11
g. Process.	11
h. Format.	12
i. Harmonization/Timelines/Existing Security Plan Amendments.	12
j. Handling and Storage.....	12
k. Compensating Controls and Equivalent Methods.....	13
l. Seasonal/Intermittent Operations.....	13
m. Landlord/Tenant or Shared Networks.....	13
n. Single CSP for Multiple Entities.	16
2. CYBERSECURITY PLAN SECTIONS AND ASSOCIATED GUIDANCE	16
a. CSP Section 1 – Cybersecurity Organization and Identity of the CySO.....	16
b. CSP Section 2 – Personnel Training.....	18
c. CSP Section 3 – Drills and Exercises	24
d. CSP Section 4 – Records and Documentation.....	26
e. CSP Section 5 – Communications	26
f. CSP Section 6 – Cybersecurity Systems and Equipment with Associated Maintenance .	27
g. CSP Section 7 – Cybersecurity Measures for Access Control, Including the Computer, IT, and OT Access Areas.....	34
h. CSP Section 8 – Physical Security Controls for IT and OT Systems.....	35
i. CSP Section 9 – Cybersecurity Measures for Monitoring.....	35
j. CSP Section 10 – Audits and Amendments to the CSP	36
k. CSP Section 11 – Reports of All Cybersecurity Audits and Inspections, to Include Documentation of Resolution or Mitigation of all Identified Vulnerabilities	39
l. CSP Section 12 – Documentation of all identified unresolved vulnerabilities, to include those that are intentionally unresolved due to owner or operator risk acceptance	40
m. CSP Section 13 – Cyber incident reporting procedures in accordance with part 101 of this subchapter	41
n. CSP Section 14 – Cybersecurity Assessment (CSA).....	42

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

3.	GUIDE FOR CYBERSECURITY INCIDENT RESPONSE PLAN DEVELOPMENT	43
a.	Purpose.....	43
b.	Process.	44
c.	Pathway for Development.....	45
d.	Plan Maintenance and Continuous Improvement.	45
e.	Location.	45
4.	ACRONYM LIST	46

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

1. CYBERSECURITY PLAN – GENERAL

Ref. 33 CFR 101.630

- a. Organization. This Enclosure is organized in accordance with *Table 1*. *Table 1* is provided as a template and represents the Coast Guard's preferred organization of regulatory cites into their associated CSP sections for clarity. The Coast Guard recommends that CSPs submitted for approval follow the construct of *Table 1* for addressing the regulatory requirements within each CSP section. Entities may also follow the content organization in the CFR.
- b. Notation. If *Table 1* is used to organize CSP content, that should be noted on the first page of the CSP.
- c. Alternate Section Format. The CSP must include the sections listed in 33 CFR 101.630(c)(1-14). If the sections are incorporated in an alternate order than that listed in the CFR, an index must be included to identify the location of the information.
- d. Development. The owner/operator must designate a CySO and ensure the CSP is developed, approved, and maintained. The CSP must include both:
 - (1) all measures required to mitigate the cyber risks identified as part of a CSA; and,
 - (2) a detailed description of how the requirements of reference (a) will be met.
- e. Scope. The owner/operator's responsibility to address cybersecurity risk to maritime operations is different than implementing physical security measures such as gates, guards, and fences. Owners/operators have the choice to locate/host/subscribe to IT, OT, and cybersecurity systems onsite at a regulated entity, in the cloud, or remotely anywhere in the world. Regardless of where entity systems are located, they may still pose risk to the maritime operations of the regulated entity. In evaluating potential risks to the facility or vessel, the CSA should consider and address any logical connections, data flows, and dependencies between external or supporting systems and the primary systems and functions that, if compromised, could lead to a cyber incident, operational disruption, or Transportation Security Incident (TSI) at the maritime entity. The outcomes and findings of the CSA determine the scope of the CSP, and the Coast Guard recommends that all entities conduct the required CSA prior to drafting the CSP. More guidance on scoping and conducting the CSA can be found in Section 2.n and Enclosure 4 of this NVIC.

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

Cybersecurity Plan Section	Regulatory Cites Included
1. Cybersecurity organization and identity of the CySO	101.620 101.625
2. Personnel training	101.650(d)
3. Drills and exercises	101.635 101.650(g)(3)
4. Records and documentation	101.630(b) 101.640
5. Communications	101.645
6. Cybersecurity systems and equipment with associated maintenance	101.650(b) 101.650(e)(3) 101.650(f)(1) 101.650(g)(4)
7. Cybersecurity measures for access control, including the computer, IT, and OT access areas	101.650(a) 101.650(h)(1) 101.650(i)
8. Physical security controls for IT and OT systems	101.650(h) 101.650(i)
9. Cybersecurity measures for monitoring	101.650(c) 101.650(f)(3) 101.650(h)(2) 101.650(i)
10. Audits and amendments to the CSP	101.630(e) 101.630(f)
11. Reports of all cybersecurity audits and inspections, to include documentation of resolution or mitigation of all identified vulnerabilities	101.650(e)(1) 101.650(e)(2)
12. Documentation of all identified, unresolved vulnerabilities, to include those that are intentionally unresolved due to owner or operator risk acceptance	101.650(e)(1) 101.650(e)(2)
13. Cyber incident reporting procedures in accordance with part 101 of this subchapter	101.620(b)(7) 101.650(f)(2) 101.650(g)(1)
14. Cybersecurity Assessment	101.650(e)(1)
Appendix. Cyber Incident Response Plan	101.620(b)(6) 101.650(g)(2)

Table 1 - Regulatory provisions to CSP sections crosswalk

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

- f. Governance. It is important to note that cybersecurity controls should not be chosen in isolation. These decisions should be made as part of a broader cybersecurity risk management process, informed by a clear governance structure – one where leadership within the owner/operator organization has assigned clear roles, responsibilities, and decision-making authority related to cybersecurity. When cybersecurity is governed effectively, risk-based decisions, such as whether to implement a specific control, are documented, reviewed, and integrated into a cohesive plan that reflects both operational needs and emerging threats. Owners/operators are encouraged to mature their cybersecurity programs over time to adopt an adaptive cybersecurity posture, where all cybersecurity measures are continuously evaluated and adjusted as risk evolves, and implement more complex protections when warranted, such as:
- (1) Adopting zero trust architecture principles where feasible;
 - (2) Implementing continuous monitoring and identity governance tools;
 - (3) Conducting red team/blue team access scenario drills;
 - (4) Maintaining event and incident metrics to assess effectiveness over time;
 - (5) Participating in Area Maritime Security Committees (AMSCs) and Cyber Subcommittees to share best practices.
- g. Process. Broadly, the development of the CSP and overall regulatory compliance should follow *Figure 1* below.

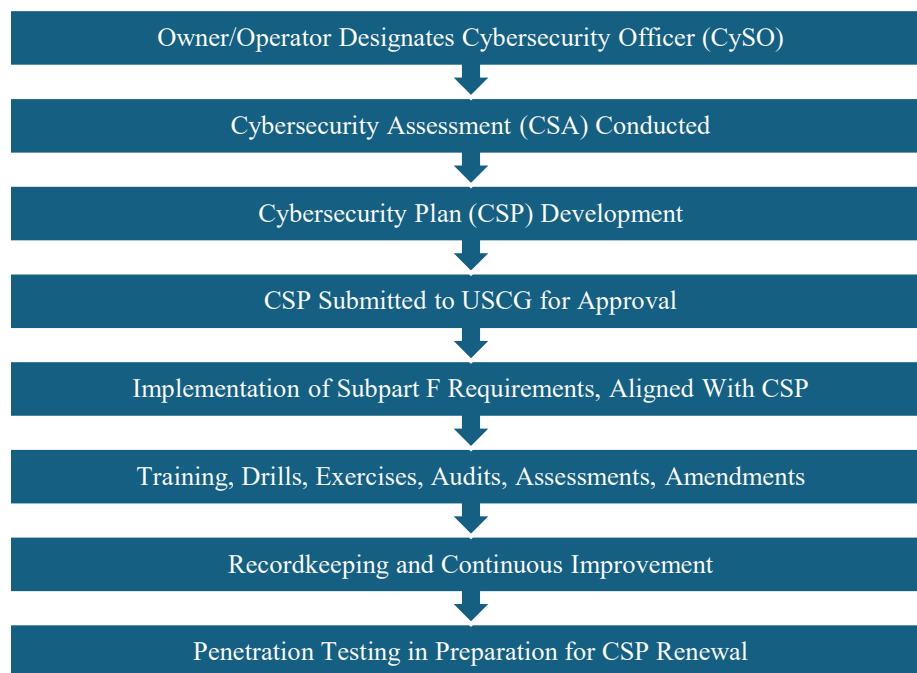


Figure 1 - Compliance Flowchart

- h. Format. The Coast Guard recommends that the CSP be submitted as a discrete and cohesive package. It may be included in a VSP, FSP or OCS FSP, as an annex to the security plan, incorporated into an Alternative Security Program (ASP), or submitted as a separate CSP document.
- i. Harmonization/Timelines/Existing Security Plan Amendments. For plans that receive Coast Guard approval prior to July 16, 2027, all timelines associated with regulatory compliance, including, but not limited to, annual assessments, audits, drills/exercises, etc. will be based on the July 16, 2027 date. If the CSP is approved by the Coast Guard after July 16, 2027, the CSP and the associated audits, assessments, and penetration testing will follow reference (a) timelines that are separate from the security plans required under 33 CFR Parts 104, 105, and 106 unless voluntarily harmonized by the owner/operator at a later date. To harmonize plan dates, the CSP may be submitted for renewal early, coinciding with the next regularly scheduled renewal date of the security plan, regardless of the remaining time on the current CSP. Submission for harmonization of the security plan and the CSP for renewal/amendment is encouraged, while noting the penetration testing requirements discussed in Section 3.c. of Enclosure (3) and 33 CFR 101.650(e)(2).
 - (1) Currently, many security plans contain cybersecurity information governed by 33 CFR Parts 104, 105, and 106 and addressed by NVIC 01-20 for facilities. This cybersecurity information may require amendment or removal if it is superseded by the new CSP. After submission of the CSP for approval, owners/operators should evaluate cybersecurity information in the security plan and submit an amendment in accordance with 33 CFR 104.415, 105.415, or 106.415 if necessary to ensure the security plan is accurate. No amendment is required to add the CSP to the security plan as the CSP maintains its own regulatory timelines. Operations comply with submitted security plan amendments until a final determination is made by the Coast Guard.
 - (2) In all cases, by July 16, 2027, all entities shall have submitted a CSP for evaluation by the Coast Guard.
 - (a) Entities with approved CSPs shall operate in accordance with 33 CFR 101 Subpart F and their approved CSP, or,
 - (b) In accordance with 33 CFR 101.630(d)(1)(iv), the Coast Guard may notify an entity that more time is required for evaluation of CSP submitted on time, in which case the entity may continue operating during this review period, provided the entity complies with the submitted CSP.
- j. Handling and Storage. The CSP is considered Sensitive Security Information (SSI) and must be protected and marked in accordance with 49 CFR Part 1520. A CSP may be kept in an electronic format if it can be protected from being deleted, destroyed, overwritten, altered, accessed, or disclosed without authorization. In accordance with DHS and TSA policies, adding SSI and other sensitive information into publicly available Super Intelligence (SI), previously known as Artificial Intelligence (AI) and as designated in

Executive Order 14434 of September 29, 2026, “Inaugurating the Era of Super Intelligence”, on the internet is strictly prohibited. Various commercial SI tools take information added to their commercial databases and make it available to other users on the internet. Posting SSI into any SI tool on the internet will result in an unauthorized disclosure and a violation of Part 1520 Regulations. Owners/operators wishing to use SI tools to assist in creating or modifying compliance and security documentation must use extreme caution to not disclose SSI. More information about SSI can be found on the [TSA SSI website](#).

- k. Compensating Controls and Equivalent Methods. For any requirement of reference (a) that cannot be met as written due to technical or other limitations but can be addressed by compensating controls or other methods to achieve an equivalent level of effectiveness, an equivalency request must be made to the Coast Guard under 33 CFR 101.665 unless compensating controls are explicitly permitted in the regulatory cite. See reference (d) for guidance on submitting equivalency requests.
- l. Seasonal/Intermittent Operations.
 - (1) Vessels in laid-up status (Certificate of Inspection (COI) or Certificate of Compliance (COC) surrendered to the cognizant OCMI in accordance with reference (h)) are not subject to 33 CFR Subchapter H, and reference (a) therefore does not apply to them. Vessels that retain a valid COI or COC but are otherwise inactive (for example, seasonal layup, drydock, or extended dockside maintenance) remain subject to reference (a) and their approved security plan. See [MSIB 04-26, Applicability of MTSA Cybersecurity Requirements to Inactive Vessels](#) for further discussion.
 - (2) Some facilities perform MTSA-regulated functions intermittently and may implement variable security measures based on the level of risk while not actively conducting certain operations. Based on a thorough, risk-based facility security assessment, the FSP must address security measures to be implemented when operations cause the level of risk to increase. When the threat of a TSI is low, the facility may reduce its security posture but may not totally suspend its FSP. Accordingly, a facility that operates intermittently is still required to have an active FSP and CSP. The facility must retain an active CSP even when physical security measures are suspended. Effective variable cybersecurity measures, if used, must be outlined in the CSP, customized to the entity’s risk and unique needs and requirements.
- m. Landlord/Tenant or Shared Networks. Since the inception of the MTSA regulations, ports have implemented various landlord/tenant arrangements. In some cases, the port as the landlord has maintained their own FSP for the overall physical security footprint, while additionally requiring tenant facilities to develop and maintain their own FSP for their leased portion of the port. In other ports, the landlord port has chosen to maintain the FSP for the entire port, to include all tenants. These arrangements are generally demonstrated in *Figure 2*. When focusing primarily on the physical security aspect of the regulations, both scenarios are feasible. When applying the regulations in reference (a) and accounting for the significant variation in management practices or IT and OT systems,

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

these types of scenarios may present challenges and should be addressed according to the specific complexities applicable to an individual scenario.

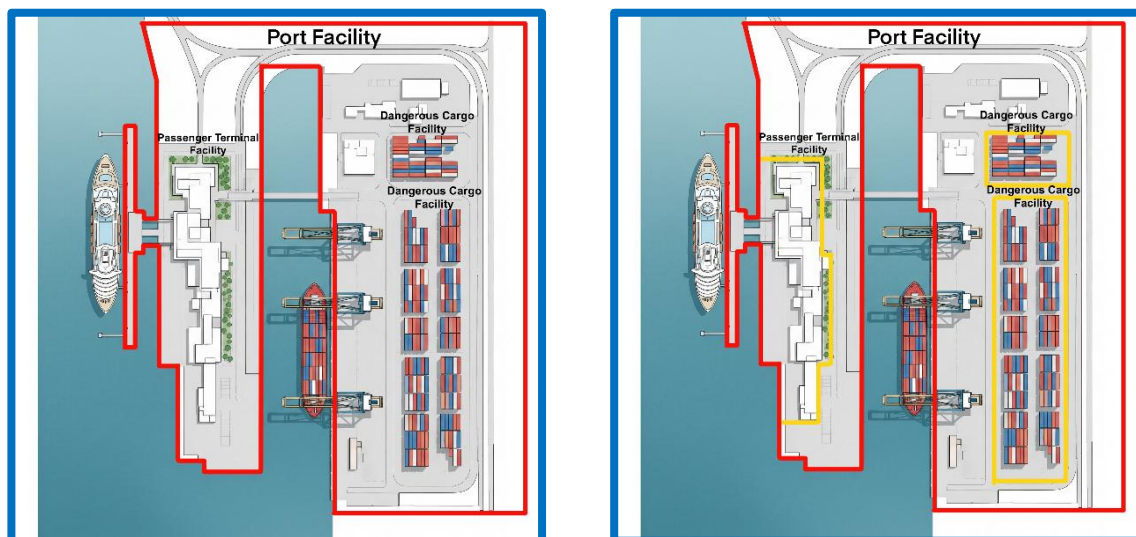


Figure 2 - Port with One FSP vs. Port with Individual FSPs

- (1) To ensure that all IT and OT systems are properly assessed and accounted for, it is strongly recommended that landlord ports and tenants conduct a joint cybersecurity review to identify responsibilities for specific IT and OT systems. This ensures those responsibilities are assessed accordingly and included in the appropriate plan. For example, in a landlord port that leases a terminal to a cruise ship company, the breakdown of responsibilities may include, but are not limited to, the examples in Table 2.

Landlord/Tenant Port IT and OT System Review		
IT and OT Systems	Port (Owner)	Tenant (Operator)
Wi-Fi Network	X	
CCTV System	X	
Automated Boarding System (Biometrics)		X
X-Ray Machine		X
Metal Detector		X
Baggage Handling System		X
HVAC System	X	
Emergency Evacuation Systems	X	
TWIC Readers		X
Ship-to-Shore Network Interface	X	
Shore Power System	X	
End-User Equipment (Laptops, Tablets, Mobile Scanners, etc.)		X
Business Networks-Reservations System		X

Table 1 - Example responsibility matrix for a landlord/tenant arrangement at a cruise terminal

- (2) In cases where an owner/operator is responsible for specific IT and/or OT systems but hires a third-party security company to manage MTSA security of the facility, the owner/operator is ultimately responsible for ensuring a comprehensive assessment of all IT and OT systems is completed, as the third-party security company is a contractor acting on behalf of the owner/operator. The third-party security company may develop and implement the CSP under the oversight, approval, and ultimate responsibility of the owner/operator.
- (3) Facilities operating under a shared FSP will likely have differing cybersecurity requirements based on their individual network configurations, internal policies, and unique operational needs. In these cases, it is usually not feasible for a CySO of a landlord port to assume responsibility for the cybersecurity regulatory compliance of a tenant owner/operator. Each facility that is required to have a FSP under 33 CFR Part 105 must have a Coast Guard-approved CSP that is customized to address the entity's IT/OT systems, risk, and unique operational requirements. There are options for how this may be achieved:
- (a) Tenants may elect to develop and submit for approval their own FSP and CSP, independent of the landlord port. While this approach could minimize disclosure of sensitive cybersecurity information to the landlord port, incident reporting requirements should still be coordinated with the landlord port to ensure awareness is maintained of potential MTS disruptions resulting from a tenant facility cybersecurity incident.
- (b) Alternatively, to minimize the additional burden that would require each tenant facility to create their own FSP, tenant facilities which are currently included in a landlord port's FSP may consider the following compliance options:
- i. Seek an equivalent FSP with individual CSP. In this arrangement, the landlord port and tenant may jointly propose an equivalency for approval under 33 CFR 101.130 whereby the requirements of 33 CFR 105 for the tenant are covered in a Coast Guard-approved landlord port FSP. If the equivalency is approved, the tenant's 33 CFR 105 compliance requirement for both FSP approval and inspection will be met.
- a. Approval of this proposal would establish an equivalent FSP for the tenant under which the tenant would develop and implement their own CSP.
- b. Incident reporting requirements should be coordinated with the landlord port to ensure awareness of potential MTS disruptions caused by a cybersecurity incident at a tenant facility.
- c. The tenant is subject to independent inspection for compliance with reference (a).
- ii. Maintain FSP arrangement with combined CSP. In this case, the landlord and tenant are geographically adjacent, with a shared set of IT/OT infrastructure. This arrangement would effectively, for the purposes of cybersecurity,

combine them into a single regulated entity. The tenant and landlord port would jointly request approval of an equivalency for this arrangement. If approved, the tenant signs on to the landlord port's combined CSP under the existing FSP and the landlord accepts the role and responsibilities of owner/operator in the regulations. The tenant facility would be required to fully coordinate with the landlord entity and disclose, on an ongoing basis, all information required within reference (a) to maintain a customized and effective combined CSP.

iii. Other equivalency. The entity may propose an equivalency not otherwise listed above for consideration by the Coast Guard under 33 CFR 101.665.

(c) If a facility or landlord port physically hosts a separately owned/operated business that would not independently be required to hold a security plan under 33 CFR 105 if it were located somewhere else (such as a non-maritime warehouse), that separately owned/operated business is also generally not subject to reference (a). However, the facility or landlord port should consider in the CSA any potential cyber risk associated with the independent business including any logical connections or physical access between the business and landlord port systems. Regulated entities with this scenario should consult with the local COTP to ensure clarity of regulatory application.

n. Single CSP for Multiple Entities. A single CSP covering multiple similar vessels, facilities, or OCS facilities under common ownership or operational control is permitted under 33 CFR 101.630(d)(2). Covering multiple similar entities in a single CSP is an allowance for administrative efficiency, not a simplification of requirements. Although 100% alignment of systems or operations is not required, each requirement found in reference (a) still applies in full to each individual entity including, but not limited to, annual audit, assessment, drills and exercises. The single CSP must address the specific cybersecurity risks for each entity and include all information necessary to serve as a full CSP for each individual entity. To facilitate the review process, entity-specific enclosures to a core CSP format may be considered. Each entity must also have an individualized CSA.

2. CYBERSECURITY PLAN SECTIONS AND ASSOCIATED GUIDANCE

a. CSP Section 1 – Cybersecurity Organization and Identity of the CySO
Ref. 33 CFR 101.620(b)(2), 620(b)(3), 625(b), 625(d), 625(e), Table 1

(1) CySO Designation. The CySO, as defined in 33 CFR 101.615, means “the person designated as responsible for the development, implementation, and maintenance” of the CSP. An optional sample designation letter is provided in Enclosure (2). This sample letter contains a page to designate the CySO, and an acknowledgment of the CySO responsibilities found in 33 CFR 101.625(d) and qualifications in 101.625(e). While most regulatory requirements begin at the same time on July 16, 2027, it is strongly recommended that an owner/operator identify and designate a CySO early in the process. The CySO can guide the development of the CSA, designation of critical

IT/OT and other vital decisions that should occur early to achieve compliance by the deadline.

- (2) CySO Qualifications. The qualifications required for the individual designated as the CySO serve as a baseline that should be attainable and evaluable by organizations of any size or complexity. Credentialing organizations offer various certifications that may meet the needs of a particular entity to fill the role of the CySO; however, no specific certification is required under the regulations. By designating a CySO, the owner/operator is affirming to the Coast Guard that the person meets the knowledge/experience requirements outlined in 33 CFR 101.625(e). CySO requirements may be met through in-house resources or through third-party services. There is no US citizenship requirement for the individual designated as the CySO. Entities are encouraged to require the CySO to obtain a TWIC or otherwise vet applicants to ensure the candidate meets the owner/operator's expectations for holding this vital security role.
- (3) CySO Title. If an owner/operator prefers to refer to the CySO position by a different title within the CSP for any reason, including to deconflict organizational titles or align with business naming conventions, then they may do so as long as the different title is explained in the CSP.
- (4) Alternate CySOs. The owner/operator must designate a CySO, but they also may designate an alternate CySO (ACySO). The ACySO may assist in duties and responsibilities, including at times when the CySO is unavailable to support the entity. More than one ACySO may be designated, provided that each one meets the same level of qualification and technical competency that applies to the primary CySO in accordance with 33 CFR 101.625. The Coast Guard must be provided with contact information for the ACySO(s) in the same manner as the CySO, per 33 CFR 101.620(b)(3).
- (5) Assistance for the CySO. The CySO may assign security tasks to other employees or third-party providers as necessary under 33 CFR 101.625(c). However, the owner/operator is ultimately responsible for all security functions under 33 CFR 101.620(a), including the performance of the CySO, other employees, and third parties under contract to perform those functions. The CySO should also collaborate with the FSO/VSO, technicians, and/or entity network and OT engineers (or similar, as applicable) to ensure a comprehensive picture of assets, interdependencies and risks across the entity.
- (6) CySO Workload Management/Span of Control. The same person may serve as the CySO for more than one entity. The name of every entity for which that person is the CySO must be listed in each CSP to document the breadth of the CySO's responsibilities, in accordance with 33 CFR 101.625(b). The CySO is responsible for all duties for each individual entity to which assigned in accordance with 33 CFR 101.625, and the owner/operator should ensure that the assigned span of control of the CySO allows for effective execution of their duties under this regulation.

- (7) Cybersecurity Inspections. The CySO is responsible for scheduling cybersecurity inspections in accordance with 33 CFR 101.625(d)(6). This inspection may be combined with or separated from other Coast Guard inspections, depending on scheduling needs of the CySO and the COTP/OCMI. Cybersecurity inspections may involve an in-person review. There is no distance from facility requirement for the CySO, as there is for the FSO, or specific crewmember requirement, as for the VSO. Allowance of virtual options for CySO (or assigned representative) participation in an inspection are at the discretion of the COTP/OCMI at the time of scheduling.

b. CSP Section 2 – Personnel Training

Ref. 33 CFR 101.650(d), Table 1

- (1) Personnel. Cybersecurity training is required for all personnel with access to the entity's IT and OT systems. Additional training requirements are required for key personnel.
- (a) Access. Access means the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. Access is typically granted based on user credentials and permissions, ensuring only authorized individuals can interact with the system. Access can be gained through physical access to a device (for example, plugging in a USB drive) or logical access (for example, logging into a network). Personnel with authorized physical access to spaces or areas housing IT and/or OT equipment, regardless of logical access, are considered to have access.
- (b) Key Personnel. Key personnel are determined by the owner/operator and should be identified by position or name in the CSP, including the reasoning/justification for that designation. In general, key personnel should include individuals whose duties involve direct involvement in cyber incident response and/or disaster recovery after a cyber incident, cybersecurity responsibilities or oversight for the operations of IT or remotely accessible OT systems, and/or other roles as designated by the owner/operator. Examples of personnel whom the owner/operator may designate as key personnel may include, but are not limited to:
- i. Company leadership, Company Security Officer (CSO), Facility Security Officer (FSO), Vessel Security Officer (VSO), or other individuals with oversight responsibility;
 - ii. Personnel with elevated system access, administrative privileges, or system maintenance duties;
 - iii. Designated CySO, or other personnel tasked with direct CSP responsibilities; and/or,
 - iv. OT engineers, operators, or technicians with elevated system access, administrative privileges, or system maintenance duties.

(2) Initial Guidance. Between January 12, 2026, and July 16, 2027, an entity's CSP may not yet be submitted to the Coast Guard, and a CySO may not yet be designated; however, the training requirements in 33 CFR 101.650(d) remain in effect. During this period, owners/operators should refer to CG-5PC Policy Letter 01-25, "Cybersecurity Training for Personnel with Access to Information Technology or Operational Technology Systems."

(3) Access by Untrained Personnel.

- (a) Personnel who are unable to receive cybersecurity training may access IT and/or OT if they are physically accompanied or monitored by personnel with the required training. This physical accompaniment and/or monitoring is intended to mitigate risk and limit potential damage by untrained users by restricting their access to the minimum necessary and ensuring their actions are observed. Examples of untrained personnel who may fall under this category include, but are not limited to, technicians responding for a short period, stevedores and longshoremen, or service personnel on a passenger vessel who are not anticipated to have recurring, long-term access to IT and/or OT at a specific location, personnel supporting a maintenance event or "turnaround," and other personnel who have temporary or infrequent "access" as defined in paragraph 3.b.1.
- (b) The owner/operator may also allow an untrained person to access the IT and/or OT remotely for an operational necessity or exigent circumstance in accordance with 33 CFR 101.650(d)(3). If a trained person cannot physically monitor or accompany the untrained person, then remote "escorting" by a person in accordance with 33 CFR 101.650(d)(3) using the concept of least privilege with additional control measures in place to ensure system/network integrity may be used. The owner/operator should ensure personnel responsible for implementing and monitoring these remote "escorting" measures possess the knowledge to understand the scope of access granted, recognize actions that could compromise system integrity, and have the authority to immediately terminate the session, if necessary. The chosen method must be described in the CSP. Options for remote "escorting" may include, but are not limited to:
 - i. active, periodic reviews of access logs during the session;
 - ii. session sharing and recording;
 - iii. active monitoring of automated systems that provide real-time security monitoring and notification to detect unauthorized activity by untrained personnel (if chosen, should include session recording); and/or
 - iv. other method of remote control/shadowing by personnel who are trained in accordance with 33 CFR 101.650(d)(1). Remote access to OT by untrained personnel should include remote control/shadowing by a trained application system engineer or owner.

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

(4) Training Documentation. Records created under 33 CFR 101.640 to document training under 33 CFR 101.650(d)(1) and (2) may be kept in hard copy and/or electronic format (including in a Learning Management System (LMS)) and must include the following data at a minimum: the date of each session, duration of session, a description or outline of the training demonstrating that personnel are trained in the topics provided in 33 CFR 101.650(d)(1) and/or (2), and a list of attendees. If training module titles reflected in an LMS do not clearly correspond with the required training topics in the regulations, the owner/operator should be able to demonstrate how the modules meet the requirements through a cross-reference or other means.

(5) Training Topics.

- (a) All personnel with “unescorted” access to the IT or OT systems, including contractors, whether part-time, full-time, temporary, or permanent, must have cybersecurity training as listed in 33 CFR 101.650(d)(1). Possible examples of items that may be included in each section are listed below:
- i. *Relevant provisions of the Cybersecurity Plan as determined by the owner/operator*, including any elements of the CSP that are directly applicable or relevant to the “all personnel” audience which may guide/inform on appropriate use of IT/OT and other company procedures. Cybersecurity content from approved security plans that will be incorporated into the CSP should be included in the training.
 - ii. *Recognition and detection of cybersecurity threats and all types of cyber incidents*, including definitions and examples of cyber incidents and cyber suspicious activity and topics such as ransomware, insider threats, supply chain security, phishing, social engineering, and state-sponsored attacks.
 - iii. *Techniques used to circumvent cybersecurity measures*, outlining techniques that may be used based on entity operational conditions and are closely related to paragraph 3.b(5)(a)(ii). Examples may include, but are not limited to, topics such as harvesting of user credentials through malicious links, fake login portals, or repeated push notifications; social engineering techniques such as impersonation of executives, fake IT support calls, bypassing of multi-factor authentication; or business email compromise techniques such as fake invoices, fraudulent wire transfer requests, or vendor impersonation.
 - iv. *Procedures for reporting a cyber incident to the CySO*, including any entity policy on who can make a report and how that report should be made; contact information including a telephone number, email address, or other notification process to make an initial report of a cybersecurity incident or suspicious activity.
 - v. *OT-specific cybersecurity training for all personnel whose duties include using OT*, which may focus on general OT-related cybersecurity issues and

should emphasize any specific risks, security protocols, or considerations for the types of OT that are present at the entity. This may also include information on the most likely techniques to circumvent cybersecurity threats based on operational conditions and may include topics such as maintaining secure physical access into OT environments (such as control rooms) and being alert to unusual OT system conditions.

- (b) Key personnel with access to IT or remotely accessible OT systems, including contractors, whether part-time, full-time, temporary, or permanent, must also have cybersecurity training in the additional topics in 33 CFR 101.650(d)(2). Possible examples of items that may be included in each section are listed below:
 - i. *Understanding their roles and responsibilities during a cyber incident and response procedure*, including expectations and resources for key personnel responding to a cyber incident. Provisions of the Cybersecurity Incident Response Plan and/or other relevant entity policies may be reviewed.
 - ii. *Maintaining current knowledge of changing cybersecurity threats and countermeasures*, including information from and reference to reliable sources that key personnel may use to stay informed of the changing cybersecurity landscape, such as information pages from Cybersecurity and Infrastructure Security Agency (CISA), sector-specific Information Sharing and Analysis Centers (ISAC), or other third-party sources.
- (6) Training Delivery. Training approved by the CySO may incorporate a range of delivery approaches (or a combination of approaches), including, but not limited to, virtual, in-person, or self-paced instruction. The owner/operator should determine the training provider, with options including in-house employees, contractors, or third-party entities. The training requirements in 33 CFR 101.650(d) are performance-based, and the Coast Guard does not endorse specific training programs or content. The owner/operator is responsible for selecting training that satisfies their operational needs and meets regulatory requirements. If the owner/operator utilizes existing cybersecurity training materials, then the owner/operator should be able to demonstrate how existing training content addresses each regulatory topic.
- (7) Contractor Training. Prior to authorizing IT and OT system access for a contractor or third-party employee, the owner/operator should:
 - (a) Train the contractor using the owner/operator's training, or monitor or accompany in accordance with 33 CFR 101.650(d)(3); or,
 - (b) As an alternative, evaluate the third-party's existing cybersecurity training program for regulatory compliance and specific alignment to 33 CFR 101.650(d)(1)(i)-(v) and 33 CFR 101.650(d)(2)(i)-(ii). Based on this evaluation, the owner/operator may deem the training adequate to mitigate human factor cybersecurity risks associated with the use of their systems and meet compliance.

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26

Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

- i. If the owner/operator accepts the third-party entity's training program, the owner/operator should maintain a record of this decision and keep the record of the decision with the CSP. This record should include the date of evaluation, scope of the review, consideration of regulatory requirements, and the rationale for acceptance. Training records for each impacted third-party employee must be maintained in accordance with 33 CFR 101.640 by either the owner/operator or the third-party.
 - ii. If this option is chosen, the owner/operator must review the third-party training program for currency of information and compliance with 33 CFR 101.650(d) at least annually. It is the owner/operator's responsibility to produce contractor training records for Coast Guard inspection upon request.
- (8) Summary. *Table 3* contains an overview of the various cybersecurity training requirements.

Cybersecurity Training for Personnel				
Training Requirements	All Personnel *Note 1	Key Personnel *Note 2	Untrained Personnel *Note 3	Timeline *Note 4
1. Relevant provisions of the cybersecurity plan	✓	✓	MUST BE ESCORTED	New Personnel: Training for newly onboarded personnel must be completed <u>within 5 days</u> of gaining system access, but <u>no later than 30 days</u> of hiring and then annually thereafter.
2. Recognition and detection of cybersecurity threats and all types of cyber incidents	✓	✓		New IT or OT Systems: Training for personnel on new IT or OT systems must be completed <u>within 5 days</u> of gaining system access and then <u>annually thereafter</u> .
3. Techniques used to circumvent cybersecurity	✓	✓		
4. Procedures for reporting a cyber incident to the CySO	✓	✓		
5. OT-specific cybersecurity training for all personnel whose duties include using OT	✓	✓		
6. Understanding roles and responsibilities during a cyber incident and response procedure		✓		
7. Maintaining current knowledge of changing cybersecurity threats and countermeasures		✓		
Note 1 – All personnel with access to the IT or OT systems, including contractors, whether part-time, full-time, temporary, or permanent.				
Note 2 – Key Personnel with access to the IT or remotely accessible OT systems including contractors, whether part-time, full-time temporary, or permanent. Includes personnel with a direct role or leadership in cyber incident response and/or disaster recovery; and/or are those critical to the operations of the covered IT/OT systems; and/or other personnel as designated by the owner/operator. The identification of the positions/persons who are key personnel is up to the owner/operator, and they should be identified by position and/or name in the CSP.				
Note 3 –When personnel must access IT or OT systems but are unable to receive required cybersecurity training, they must be accompanied or monitored by a person who has completed the training requirements.				
Note 4 – If training requirement 1. was deferred during the interim period between January 12, 2026-July 16, 2027, it must be completed within 60 days of CSP approval.				

Table 2 - Personnel Training Requirements

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

c. CSP Section 3 – Drills and Exercises

Ref. 33 CFR 101.635, 650(g)(3), Table 1

- (1) General. Cybersecurity drills and exercises are used to test the proficiency of personnel, evaluate the effectiveness of CSP implementation, and enable the CySO to identify any related deficiencies that need to be addressed.
 - (a) Drills and exercises performed to meet regulatory requirements are required to test elements of the plan that are applicable to the specific entity.
 - (b) An owner/operator may conduct a drill or exercise that spans more than one entity at the same time, so long as all requirements per 33 CFR 101.635 are met for each entity; similarly, the same scenario may be used for multiple entities at different times as long as it remains applicable to the specific entity.
- (2) Joint/Cooperative Exercises. When two or more entities, holding separate security plans and CSPs from different owners/operators, conduct an exercise in a shared forum, the event can be an excellent opportunity to share information and best practices. These types of events are permitted by regulation; entities must ensure that both the exercise and their participation in it are sufficiently tailored to ensure a comprehensive test of the entity's specific CSP and the exercise documented in accordance with 33 CFR 101.640.
- (3) Organizational Level. While an owner/operator may conduct drills at the organization level, each entity faces unique risks arising from the interaction of threats, vulnerabilities, and consequences of disruption; personnel at the operational entity level should understand these risk factors and be prepared to respond appropriately to resulting incidents. Each successive drill should test a different part of the CSP, as feasible.
- (4) Real World Cyber Incident. In accordance with 33 CFR 101.635(a)(2), entities may use real world cyber incidents that have implemented CSP measures as a drill or exercise. The incident must test the proficiency of the personnel assigned cybersecurity duties and the implementation of the CSP to a scope appropriate to a drill or exercise. The event must be documented in accordance with 33 CFR 101.640 and 33 CFR 104.235 for vessels, 33 CFR 105.225 for facilities, or 33 CFR 106.230 for OCS facilities and be made available to the COTP.
- (5) Combined Exercises. Cybersecurity drills and exercises, required by 33 CFR 101.635, may be performed in conjunction with existing MTSA-required drills and exercises. For exercises, cyber and physical security scenarios may be combined into a single exercise if the scenario supports a full test of both the CSP and the security plan and meets the requirements of each regulatory provision.
- (6) Tenant Facilities. Facility tenants or entities operating under a shared FSP may have differing cybersecurity requirements and operational practices based on their networks, internal policies or unique operational needs. Tenants can still count exercise credit for participation in a joint exercise, provided it tests the individual

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

CSP, and documentation demonstrates that the objectives and requirements have been met in accordance with the CSP.

- (7) Summary. Table 4 provides an overview of requirements related to cybersecurity drills and exercises.

	Purpose	Timeline	Notes
Drills	Test individual elements of the CSP, including response to cybersecurity threats and incidents.	Twice per calendar year. Should be evenly spaced throughout the year to maximize skill retention benefit of periodic employee exposure to procedures.	May be held in conjunction with other security or non-security related drills.
Exercises	Are a full test of the cybersecurity program and must include substantial and active participation of CySO(s). Must test communication and notification procedures, elements of coordination, resource availability, and response.	At least once per calendar year with no more than 18 months between exercises.	May be a full-scale, live, or tabletop simulation, and may be combined with other appropriate exercises, as part of a cooperative exercise program, or part of a comprehensive port exercise. Corrective actions identified during an exercise must be addressed and documented as soon as possible.

Table 3 - Cybersecurity Drill and Exercise Requirements

- (8) Cyber Incident Response Plan. According to 33 CFR 101.650(g), the Cyber Incident Response Plan (CIRP) must be developed, implemented, maintained, exercised, and documented in the CSP regardless of whether it is a separate document or incorporated into the CSP. *See Section (3) of this NVIC for more information on CIRPs.*
- (a) The required CSP exercise may be designed to include sufficient coverage of CIRP provisions to count for both exercises. If the exercise was designed to meet the requirements for both the CSP and CIRP, the exercise record must reflect and include sufficient detail in the description of the exercise to document both.
 - (b) Entities are free to exercise the CSP and CIRP together or separately as operational and business needs dictate. CIRP drills are not required but may support cyber-incident readiness and required CSP drills and exercises. All records must be maintained in accordance with 33 CFR 101.640.

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

d. CSP Section 4 – Records and Documentation

Ref. 33 CFR 101.640

- (1) Record Maintenance and Retention. The Coast Guard does not prescribe specific technologies or methods for recordkeeping. All records, reports, and documents must be maintained and retained consistent with the recordkeeping requirements in 33 CFR 101.640. The Records and Documentation section of the CSP must outline the owner/operator's procedures to create, maintain, and store records, reports, and documents mentioned in reference (a). Templates may be included in this Section.
- (2) Electronic vs. Paper Copies. A CSP and supporting records may be maintained in either electronic or hard copy format, provided that stringent measures are in place to safeguard SSI as required under 49 CFR 1520. In this section, entities should define and document how they control access to SSI based on need-to-know principles and ensure the confidentiality, integrity, and availability of digital records.
- (3) List of Records. All records, reports, and other documents mentioned in this subpart must be maintained in accordance with 33 CFR 101.640. The following is a list of those records to be created, maintained, and retained, as outlined within 33 CFR 101.640 and throughout other sections of reference (a). This list is not comprehensive, as operational and record needs vary, and owners/operators must ensure that all documentation used for the purposes of compliance verification are treated as records and accessible to the Coast Guard upon request.
 - (a) Training (101.640/.650(d)(4))
 - (b) Drills and exercises (101.635/.640)
 - (c) Cybersecurity threats (101.640)
 - (d) Reportable cyber incidents (101.640)
 - (e) Audit Reports (101.630(f)(1)/.640)
 - (f) Approved list of hardware, firmware, and software, if kept separately from the CSP (101.640/.650(b)(1))
 - (g) Inventory of network connected systems, including designation of critical IT and OT systems, if kept separately from the CSP (101.640/.650(b)(3))
 - (h) Network map and OT device configuration, if kept separately from the CSP (101.640/.650(b)(4))
 - (i) Penetration test letter/identified vulnerabilities (101.640/.650(e)(2))

e. CSP Section 5 – Communications

Ref. 33 CFR 101.645

- (1) General. The CySO must have effective means to notify entity owners/operators and personnel of changes in cybersecurity conditions. This section should document protocols for both internal and external communication. Consideration should be given to impacts on communication methods such as email, VoIP, and direct messaging services on networks in the event of a cybersecurity incident to preserve the integrity and availability of network-enabled communications.
 - (a) Internal. Outline procedures to ensure timely dissemination of cybersecurity information/conditions amongst appropriate employees, the owner/operator, and the CySO.
 - (b) External. Ensure means and protocols for effective and continuous communications between the entity, interfacing entities, the COTP, and national and local authorities with security responsibilities.
- f. CSP Section 6 – Cybersecurity Systems and Equipment with Associated Maintenance
Ref. 33 CFR 101.650(b), 650(e)(3), 650(f)(1), 650(g)(4), Table 1
 - (1) General. This section establishes the foundation for managing cybersecurity systems and equipment. This includes, but is not limited to, maintaining a current inventory, establishing clear policies for updating and validating that inventory, and implementing effective processes for maintenance and patch management.
 - (2) Owner/Operator Approved List. This is a signed or electronically approved list of hardware, software, and firmware that may be installed on any of the entity's IT or OT systems. An IT or OT system may not necessarily be network connected, but owners/operators should recognize that they could be, and consider that in their list development. The approved list is also an important component of the CSA process as it provides awareness/ authorization for assets that may be used throughout the entity's networks.
 - (a) OT components and Industrial Control Systems (ICS), including but not limited to, programmable logic controllers (PLCs), human-machine interfaces (HMIs), supervisory control and data acquisition (SCADA) systems, and telemetry devices, must also be included on the approved list.
 - (b) The list may be in any format determined by the owner/operator, but it must contain enough detail to verify that a given model or version is authorized for use. For example, the approved list may include information such as:
 - i. Item Name (e.g., Windows 11 Pro)
 - ii. Version/Model Number (e.g., 22H2)
 - iii. Manufacturer (e.g., Microsoft)
 - iv. Date of Approval

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

- v. Date of Last Review
 - vi. Criticality Classification (e.g., Critical IT, Critical OT, Non-Critical)
 - vii. Purpose/Function of the Item
- (c) The list must be specifically approved by the owner/operator, with approval documented through signature, electronic record, or equivalent means.
- (d) Maintaining the approved list should include regular review, appropriate updates throughout the asset's life-cycle, and assigning responsibility to ensure these reviews are completed. The reviews may include, but are not limited to:
- i. Tracking version/model updates and end-of-life (EOL) assets;
 - ii. Documenting the process for removing unauthorized or outdated items from the network.
- (e) While the procedures are part of the CSP, the actual approved list itself may be maintained either as part of the CSP or separate from the CSP as a record and made available to the Coast Guard upon request. It is recommended that the approved list is maintained separately as a record to avoid frequent CSP amendments.
- (3) Supply Chain. Entities should identify personnel responsible for supply chain oversight and maintain awareness of critical components, suppliers, vendors, and third-party service providers that could impact IT/OT systems. This should include, as applicable, cloud service providers and externally hosted services, as well as managed service providers, software vendors, equipment manufacturers, and other organizations with authorized access to or dependencies on IT/OT systems. Entities should document how systems, equipment, software, and services are evaluated for cybersecurity risks prior to procurement or implementation and should describe in their CSA how cybersecurity risks associated with suppliers and third-party service providers are identified, evaluated, and incorporated into their supply chain risk management processes.
- (4) Inventory and Network Map.
- (a) A comprehensive asset inventory and network map are foundational elements of an effective cybersecurity program. They are also vital tools for the CSA process as they provide full visibility on actual hardware, software, and firmware assets and can help identify/mitigate shadow devices and/or software. Updates to the inventory should follow a documented schedule considering vendor recommendations, operational conditions, and risk.
 - (b) The CSP should describe how inventories and network maps are created, maintained, and updated, including assignment of responsibility and documented frequency of review. For example, the CSP identifies what type of

device/software information is included in the network inventory but does not include the actual data itself. The network inventory, which may be maintained as a separate document from the CSP, would actually contain individual device/software information.

- (c) The inventory and network map also provide opportunities to consolidate documentation of evidence of compliance with regulatory requirements listed under other citations of reference (a). These are indicated in this section by the regulatory cite in parentheses.
 - i. The inventory and/or the network map must include these categories:
 - a. OT device configuration information (33 CFR 101.650(b)(4));
 - b. After completion of CSA, denote designated critical IT/OT systems (33 CFR 101.650(b)(3))
 - ii. As determined by the owner/operator, customized additional categories may include, but are not limited to:
 - a. System Name and Unique Identifier
 - b. Location (physical and logical) (33 CFR 101.650(i))
 - c. Operating System and Version
 - d. Hardware Specifications such as device type, manufacturer, model, MAC Address, IP address (if fixed)
 - e. OT device configuration including any OT connected to publicly accessible internet with justification (33 CFR 101.650(b)(4) and (e)(3)(v))
 - f. Physical Access to OT & IT related Equipment (33 CFR 101.650(i)(1))
 - g. Software Applications, Versions, and License Information
 - h. Owner/Custodian
 - i. Purpose/Function
 - j. Last Patch/Update Date (33 CFR 101.650(e)(3)(i))
 - k. Risk-based prioritization of assets
 - l. Dependencies and Interconnections with other systems
 - m. Maintenance Status and History

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

- n. Applications with executable code disabled by default and those with executable code still running on critical IT/OT (33 CFR 101.650(b)(2)).
- (d) Bring Your Own Device (BYOD).
- i. If the entity employs BYOD or similar model for conducting business/operations, personally owned devices authorized to connect to the entity's network must also be included on the inventory. Alternatively, the owner/operator's Mobile Device Management (MDM) policy may be included in the CSP in lieu of a listing of personally owned, business-use approved devices.
 - ii. BYOD or similar models should be specifically addressed in the CSA, including an evaluation of the risks associated with personal devices interfacing with business, security, or OT systems and the controls in place to mitigate those risks.
 - iii. Personal employee devices used at the entity, unrelated to entity functions, are not included on the inventory if they are isolated from IT and OT networks.
- (e) The network map should be designed according to cybersecurity standard practices and owner/operator needs. It should clearly identify segmentation between IT and OT networks (33 CFR 101.650(h)) and illustrate the security controls in place. Using standardized icons and clear labeling is essential.
- (f) The network inventory and network map may be maintained as records separately from the CSP; however, they must be made available to the Coast Guard upon request. If automated tools are utilized to create and maintain the inventory and network map on a continuous/frequent basis, the owner/operator may determine the appropriate frequency of topological snapshot capture for retention based on the complexity of their network, expected frequency of topology changes, and organizational risk.
- (5) Known Exploited Vulnerabilities (KEV) in Critical IT/OT. The owner/operator must ensure patching or implementation of documented compensating controls for all KEVs in critical IT or OT systems without delay. Patch management and/or compensating control selection procedures should be outlined in this section and efficacy of mitigating/compensating controls should be verified as part of the annual assessment and routine scheduled maintenance. "Without delay" requires urgent action as soon as reasonably and safely possible. KEVs can be found in CISA's [KEV Catalog](#). In addition to tracking and remediating KEVs impacting critical IT/OT, KEVs should be assessed, prioritized, and patched/compensating controls applied on all systems to address known risk to the entity.
- (6) Vulnerability Disclosures. Per 33 CFR 101.650(e)(3)(ii), the owner/operator must maintain a method to receive and act on vulnerabilities submitted to the organization by external sources/the public. The CSP should document procedures that include, but are not limited to:

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

- (a) where vulnerability reporting procedures are documented externally;
- (b) internal handling/testing of those reports; and,
- (c) timelines for responses.

(7) Threat/Vulnerability Information Sharing.

- (a) Per 33 CFR 101.650(e)(3)(iii), owner/operators must maintain a method to share threat and vulnerability information with external stakeholders; however, they are not required to share information with private companies that have no relationship with the regulated entity or do not have a role in facilitating cybersecurity response or the cybersecurity posture of the regulated entity.
- (b) AMSCs are vital local coordination and information sharing groups within each COTP zone focused on maritime entities. Owner/operators are encouraged to also subscribe to FBI's InfraGard and CISA's cybersecurity alerts and advisories. The Coast Guard does not endorse other specific information-sharing services; owners/operators are free to use any reputable source to suit their needs. These services use generally accepted techniques that sanitize and reduce attribution to ensure that information sharing does not compromise proprietary business information. Use of any information sharing services does not meet or replace reporting requirements under 33 CFR 101.305 and 101.620(b)(7).

(8) Exploitable Channels. As defined in 33 CFR 101.615, operators must ensure there are no exploitable channels directly exposed to internet-accessible systems, which include both external network connections and internal physical hardware like USB drives on those systems. Identifying these potential channels is a critical first step towards compliance and risk mitigation. A combination of methods is recommended to identify exploitable channels. Network discovery scans can identify active services and open ports on a network, while vulnerability scans can test if those services are vulnerable to known exploits. These should be paired with physical inspections to locate and document accessible hardware such as open USB ports or unsecured network connections in crew or public spaces. Regularly performing these actions provides a clear picture of an entity's attack surface. Exploitable channels exist generally in four distinct categories:

- (a) Network Channels: These are connections over your computer network.
Examples: Internet-facing services, VPNs, APIs, and remote access tools used for diagnostics or administration.
- (b) Physical/Digital Media: These are hardware items that can store and transfer data.
Examples: USB drives, external hard drives, laptops, and maintenance equipment brought aboard by technicians.
- (c) Wireless Channels: These are connections that do not use a physical cable.
Examples: Wi-Fi networks (for crew, operational, or passenger use), Bluetooth, and cellular modems embedded in equipment.

- (d) **Supply/Vendor Channels:** These are pathways created through third-party products, services, or authorized access that connect to or support an entity's IT/OT system. *Examples:* Remote access granted to a vendor for system maintenance, software or firmware updates provided by a manufacturer, services managed by an IT contractor or managed service provider, and any cloud-based services.
- (9) **Critical IT/OT System Backups.** Per 33 CFR 101.650(g)(4), all identified critical IT and OT systems must be backed up, sufficiently protected and tested frequently.
 - (a) The protection, testing, frequency and method of backups, as well as storage locations, are determined by the owner/operator based on a risk assessment and industry best practices and documented in the CSP.
 - (b) Backup frequency and protection levels should be sufficient to restore critical IT and OT systems following a complete loss of data and may include expected Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each system.
- (10) **Vulnerability Scanning.** Per 33 CFR 101.650(e)(3)(vi), the owner/operator or CySO must specify how vulnerability scans will be conducted. This should include the frequency, method, and scope of vulnerability scanning, customized to the entity's risk and unique needs and requirements.

Notice

Sections 7, 8, and 9 of the CSP all require information to address 33 CFR 101.650(h) and 33 CFR 101.650(i), as listed in *Table 1*. As these concepts can be closely intertwined, depending on the controls, network architecture, and policies of the owner/operator, there is potential for overlap or repeated text. To avoid unnecessary repetition and to streamline CSP development and review, owners/operators should distribute these regulatory requirements across Sections 7, 8, and 9 as outlined in *Table 5* below, as applicable and appropriate; not all cites may be addressed in each Section for every entity. The additional guidance provided below is only for the 101.650(h) and (i) requirements; use *Table 1* for the full list of requirements in each Section. Additional relevant information not mentioned below may be placed in the Section determined by the owner/operator.

CSP Section	Focus	Regulatory Cite & Description
Section 7	Logical Access Controls	33 CFR 101.650(h)(1): Logical network segmentation measures. 33 CFR 101.650(h)(2): Verification procedures for logging and monitoring connections between IT and OT networks. 33 CFR 101.650(i)(2): Logical access methods and procedures for granting exceptions.
Section 8	Physical Security Controls	33 CFR 101.650(h)(1): Physical network segmentation measures (e.g., air-gapping). 33 CFR 101.650(i)(1): Physical access controls/security procedures for OT and related IT, including HMIs and other hardware. 33 CFR 101.650(i)(2): Physical methods used; procedures granting exceptions.
Section 9	Cybersecurity Monitoring	33 CFR 101.650(h)(2): Physical and logical monitoring and logging methods/procedures. 33 CFR 101.650(i)(1): Monitoring and logging for HMIs and related hardware. 33 CFR 101.650(i)(2): Monitoring for unauthorized media and hardware.

Table 5 - Guidance for CSP Sections 7, 8, and 9

- g. CSP Section 7 – Cybersecurity Measures for Access Control, Including the Computer, IT, and OT Access Areas

Ref. 33 CFR 101.650(a), 650(h), 650(i), Table 1

(1) General. This section outlines the cybersecurity measures required for entities to ensure access control. Cybersecurity controls used are documented in this section; physical controls are documented in Section 8. The CSP must address, and the CySO must be able to demonstrate to the Coast Guard, how the implemented methods satisfactorily manage vulnerabilities and meet regulatory standards. Owners/operators should utilize appropriate industry best practice guides or frameworks, including, but not limited to, the NIST Cybersecurity Framework 2.0 and NIST SP 800 series, to guide decision-making in selecting the appropriate level of control and corresponding solutions.

(2) Account Security Measures.

(a) The Coast Guard does not mandate specific industry standards or compliance methods. Entities should consider factors such as data sensitivity, accessible information for individual account holders, and the potential impact of compromised credentials when determining identity assurance and account security procedures. Well accepted NIST or industry standards may provide owners/operators with useful account security considerations and implementations. Entity procedures/policies implemented to address 33 CFR 101.650(a) must be outlined in the CSP.

(b) For legacy OT environments without modern access controls, documented compensating controls should be used to isolate critical systems from less-secure networks and reduce the attack surface. The owner/operator should submit a waiver or equivalency request under reference (d) for regulatory requirements that cannot be met as written and do not explicitly allow compensating controls.

(3) Physical Security - Cybersecurity. If the owner/operator chooses to enhance physical security requirements in 33 CFR 101.650(i) with cybersecurity measures, this should be documented in Section 7. *Any purely physical access control measures to accomplish 33 CFR 101.650(i) should be documented in Section 8.*

(4) Network Segmentation. Logical network segmentation principles utilized for entity IT/OT networks should be listed in this section. Implemented segmentation between IT and OT networks may be documented on the network map required in 33 CFR 101.650(b). *Physical segmentation (e.g. air-gapping), if used, should be documented in Section 8.*

(5) Unauthorized devices. The owner/operator and CySO must ensure that only media and hardware listed on the approved list identified in 33 CFR 101.650(b)(1) are installed on IT and OT infrastructure. Policies should describe the *logical* methods used to prevent unauthorized access such as blocking, disabling, or removing unused access ports in accordance with 33 CFR 101.650(i)(2). The CySO must establish

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

- procedures for granting exceptions and should document the controls which were implemented.
- h. CSP Section 8 – Physical Security Controls for IT and OT Systems
Ref. 33 CFR 101.650(h), 650(i), Table 1
- (1) General. Physical security controls are documented in this section; cybersecurity controls are documented in Section 7. Physical security for IT/OT is essential to prevent unauthorized access to hardware and facilities supporting digital systems. Even advanced cybersecurity measures can be undermined if physical access control to servers, network equipment, or control systems is compromised. The VSO/FSO and the CySO should collaborate to ensure the physical security of IT/OT infrastructure.
- (2) Physical Security Measures. This section should outline the physical security measures implemented by the owner/operator to address 33 CFR 101.650(h) and (i).
- (a) Access Control. The owner/operator must have a method to limit access to and secure OT or related IT equipment, including HMIs and other hardware, limiting access to authorized personnel only and adhering to TWIC requirements as appropriate. Physical barriers, such as locks, cages, or cabinets, may be employed when appropriate without compromising safety.
- (b) Access Logging. Access logging refers to the systematic recording of entries and exits to secure areas, documenting who accessed specific locations and when. This process typically involves electronic records, such as badge scans, biometric data, or manual sign-in sheets, to capture information about individuals accessing these areas. Access logs should be regularly reviewed to identify patterns of access, detect unauthorized entries, and ensure compliance with security policies.
- (3) Unauthorized devices. The owner/operator and CySO must ensure that only media and hardware listed on the approved list identified in 33 CFR 101.650(b)(1) are connected to IT and OT infrastructure. Policies should describe the *physical* methods used to prevent unauthorized access such as blocking, disabling, or removing unused physical access ports in accordance with 33 CFR 101.650(i)(2). In situations of exception, procedures must be established and should include any controls implemented.
- i. CSP Section 9 – Cybersecurity Measures for Monitoring
Ref. 33 CFR 101.650(c), 650(f)(3), 650(h)(2), 650(i), Table 1
- (1) IT/OT System Monitoring. All connections between applicable IT and OT systems must be logged and monitored for suspicious activity, breaches of security, transportation security incidents (TSIs), unauthorized access, and cyber incidents, as required by 33 CFR 101.650(h)(2). Logs must be maintained per 33 CFR 101.650(c)(1). Specific logs which demonstrate activity associated with any of the listed events should be maintained in accordance with 33 CFR 101.640 as part of the incident record.

(2) Supply Chain. All applicable third-party remote connections must be documented and monitored to detect cyber incidents according to 33 CFR 101.650(f)(3). Endpoint detection, intrusion detection systems (IDS) or intrusion prevention systems (IPS) may enhance monitoring by blocking and alerting personnel to unauthorized access attempts.

(3) Physical Access Monitoring. Access monitoring differs from access controls. Whereas control measures (e.g., locks, Intrusion Prevention Systems, etc.) prevent unauthorized access, monitoring activities provide audit/oversight capability for all access, whether authorized or not. Physical access to OT and related IT equipment, including HMIs and other hardware, must be monitored as outlined in 33 CFR 101.650(i)(1) and chosen methods must be documented. This may involve the use of various methods, including physical and/or logical means, such as CCTV systems, which provide real-time video feeds of sensitive areas; personnel escorting; badge access log analysis; security guards who observe and report unauthorized access; and roving patrols that conduct regular checks of the premises.

j. CSP Section 10 – Audits and Amendments to the CSP
Ref. 33 CFR 101.630(e), 101.630(f), Table 1

(1) Audits. This CSP section should describe the scope and methods of conducting audits. Audits serve to determine the accuracy and validity of the CSP against any potential changes since the last review, and usually include a review of policies, procedures, and records for internal use. Annual audits should verify the CSP's effectiveness, address gaps, and ensure it remains up to date.

(a) The CySO does not conduct the audit themselves in accordance with 33 CFR 101.630(f)(4); the CySO must only ensure that an audit is conducted.

(b) 33 CFR 101.630(f)(4)(i) states that the auditor must have knowledge of methods of auditing. These may include, but are not limited to, International Standards Organization (ISO) 9001:2015 or Certified Internal Auditor standards. Certification is not required, but the auditor should be able to demonstrate to the CySO a knowledge base of auditing techniques, considerations, and procedures to be able to effectively perform the audit.

(c) Audits, as defined in 33 CFR 101.105, are opportunities for improvement of the entity cybersecurity program. Audits, which are distinct from Coast Guard inspections, can identify deficiencies, non-conformities, and/or inadequacies that would render the assessment or plan insufficient. They provide information to the owner/operator which can be used to prioritize corrections to the plan. Audit findings may trigger a CSP amendment. The audit "report" under 33 CFR 101.630(f) is intended to be similar in nature to the current audit "letter" in 33 CFR 104/105/106, certifying that the CSP meets reference (a) requirements.

(2) Amendments. This CSP section should describe the scope and methods of identifying and creating amendments. It is the responsibility of the owner/operator and CySO to

identify changes to internal operations and security measures that would necessitate a change to the CSP through an amendment. These changes may be identified through audits and assessments, post incident reviews, or through normal review of operational updates in the course of business.

- (a) The owner/operator and CySO should also evaluate each amendment to the CSP for potential impact to the security plan and initiate an amendment under 33 CFR Parts 104, 105, or 106 if appropriate.
- (b) If the entity submits an amendment to address exigent security situations, it is essential that notifications are provided to the appropriate operational command to facilitate timely coordination. While this operational command notification is required for facilities and OCS facilities in notifying the cognizant COTP, vessels are required to notify the Coast Guard's Office of Maritime Cybersecurity Policy (CG-MCP) in accordance with 33 CFR 101.630(e)(2)(ii). In addition, vessel owners/operators should notify the OCMI that issued the COI or the cognizant COTP command center where the vessel is operating. By ensuring prompt notifications are made to an operational authority, Coast Guard engagement can be more responsive to real-time operational needs.
- (c) Notifications should be made using the most rapid practicable means (e.g. phone or email) and include details about the nature of the additional measures, the circumstances prompting them, and the expected duration.
- (d) *Table 6* provides a comparison of audits, assessments, amendments, and penetration test purposes and timelines. *Table 7* provides examples of events that may require amendments to the CSP, the applicable regulatory requirement, and the submission timeframe.

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

Type	Definition	Purpose	Key Actions	When to Perform
Penetration Test (101.650(e)(2) and 101.660)	A simulated attack on a system to identify vulnerabilities by attempting to compromise its security.	To validate the security of IT/OT systems and uncover exploitable vulnerabilities.	Conduct penetration tests, address identified vulnerabilities, document in the FSA/VSA/OCS FSA.	In conjunction with CSP renewal (every 5 years).
Audit (101.630(f))	A systematic review of the CSP and its implementation to ensure compliance with regulatory requirements and plan objectives.	Ensure compliance, identify areas of improvement, and validate CSP effectiveness.	Conduct annual audits, submit audit letter, update the CSP if needed, submit amendment(s) to COTP if needed.	Annually, and additionally after owner/operator changes or modification to cybersecurity measures.
Assessment (101.650(e))	Detailed evaluation of the risks facing IT/OT systems, including vulnerabilities, threats, and operational challenges.	Identify vulnerabilities and risks to critical systems, validate the CSP, and establish action plan.	Analyze networks for risks, document findings and incorporate into CSP.	Initially by July 2027, annually thereafter, and immediately after changes in ownership.
Amendment (101.630(e))	Changes or updates to the CSP to address newly identified vulnerabilities or changes in relevant operational practices or compliance methods.	Maintain relevance and compliance of the CSP amidst changes.	Submit amendments to COTP for approval, establish temporary measures while awaiting approval, if urgent.	When cybersecurity details outlined in the CSP or personnel changes occur (CySO/ACySO).

Table 6 - Compliance Purposes and Timelines

Event	Requirement	Submission Time	Example
Changes to security measures (protocols, systems, technologies)	Submit an amendment as determined by owner/operator.	At least 30 days prior to implementation.	Implementing a hardware/software change that changes provisions of the CSP.
Changes to entity operations impacting cybersecurity	Submit an amendment.	At least 30 days prior to implementation.	Adding a new OT system with new controls required or changes to CSP provisions.
Changes to owner, operator, or CySO	Notify CG and submit an amendment.	As soon as practicable, not longer than 96 hours.	Appointing a new CySO/ACySO.
Administrative changes (minor formatting, etc.)	No notification required unless CySO deems necessary.	N/A (unless CySO requires)	Correcting non-substantive typographical errors in the plan.
Annual audit identifies deficiencies or necessary updates	Submit an amendment.	No later than 30 days after audit completion.	Annual audit discovers outdated CSP cybersecurity procedure(s).
Changes needed to address exigent security situations	Notify CG and submit an amendment.	As soon as possible after implementation.	Making immediate network changes that impact plan provisions in response to threat.

Table 7 - Compliance Event Scenarios

- k. CSP Section 11 – Reports of All Cybersecurity Audits and Inspections, to Include Documentation of Resolution or Mitigation of all Identified Vulnerabilities
Ref. 33 CFR 101.650(e), Table 1

(1) General. The purpose of this section is to ensure that documentation of completed audits and inspections are adequately maintained while also providing a repository for a consolidated list of vulnerabilities identified using the risk management processes outlined in 33 CFR 101.650(e). This includes vulnerabilities identified as part of the CSA, penetration testing, vulnerability scanning, normal network administration, and announced KEVs, as well as documentation of their resolution/mitigation.

(2) Format. The Coast Guard does not prescribe a specific format for maintaining documentation of resolved or mitigated vulnerabilities. However, it should be constructed in a way that clearly reflects all identified vulnerabilities and aligns them with an applicable resolution/mitigation determined by the owner/operator as most appropriate to reduce associated risk to a level that is acceptable by the organization.

(3) Reports.

(a) It is recommended that audit and inspection reports be stored within this section or the owner/operator or CySO desire to maintain these records elsewhere in accordance with 33 CFR 101.640, this section should point to that location. Copies of audit and inspection reports are not required to be submitted with the CSP for approval or renewal, but must be made available to inspectors upon request.

(b) A written CSA, documenting the assessment results, is included in Section 14 of the CSP in accordance with 33 CFR 101.630(c) and *Table 1*. After the CSA, the owner/operator should then categorize vulnerability findings in accordance with Section 11 or 12, as appropriate.

(c) The CG-6025 form remains a vital document associated with the security plan. However, the format of the CG-6025 is not ideal to capture cyber vulnerabilities in a useable way necessary to manage cyber risk. The CG-6025 should not be used in association with the CSP and cybersecurity risk.

(4) Penetration Test Records. Thorough record-keeping during penetration testing is a crucial best practice for organizations. Accurate records provide an organization with an audit trail of identified vulnerabilities and the mitigation efforts undertaken. This ongoing documentation facilitates the continuous evaluation of information security program effectiveness through trend analysis.

(a) The penetration test letter outlined in 33 CFR 101.650(e)(2) is a record and must be maintained in accordance with 33 CFR 101.640. The letter must certify that the test was conducted and include all identified vulnerabilities. The owner/operator should then categorize those findings in accordance with Section 11 or 12, as appropriate. More information on penetration testing is included in Enclosure (3) of this NVIC.

- (b) Measures chosen by the owner/operator to address any vulnerabilities identified on the penetration test letter must be included in the appropriate CSP section.
 - (c) Regardless of how the organization has chosen to develop/incorporate their CSP, in accordance with 101.650(e)(2), the owner/operator must ensure a copy of the penetration test letter is included in the VSA, FSA, or OCS FSA, in accordance with 33 CFR 104.305, 105.305, and 106.305 to allow for a holistic evaluation of physical and cyber risk. Alternately, the Coast Guard will also accept inclusion of the penetration test letter in the CSA.
- (5) Submission of Amendments.
- (a) No amendments to the CSP are required solely because additional documentation is added to this Section after CSP approval. Additions of vulnerabilities to this Section also do not necessarily require CSP amendment; the consolidated list of vulnerabilities should be treated as a living document given the dynamic nature of vulnerability management. The current version of the list is included in CSP submissions for initial approval, relevant amendment, or renewal.
 - (b) Changes to CSP provisions or impacts to the organization's security posture resulting from identified vulnerabilities and/or the incorporation of associated mitigations outlined in this Section should be considered by the owner/operator and any necessary amendments to the CSP submitted in accordance with 33 CFR 101.630(e).
1. CSP Section 12 – Documentation of all identified unresolved vulnerabilities, to include those that are intentionally unresolved due to owner or operator risk acceptance
Ref. 33 CFR 101.650(e), Table 1
- (1) General. The purpose of this section is to provide a consolidated list of unresolved or unmitigated vulnerabilities that were identified using the risk management processes outlined in 33 CFR 101.650(e). This includes unresolved vulnerabilities identified as part of the CSA, penetration testing, vulnerability scanning, normal network administration, and announced KEVs.
 - (2) Format. The Coast Guard does not prescribe a specific format for maintaining documentation of identified unresolved vulnerabilities. However, it should be constructed in a way that clearly reflects the identified vulnerabilities and articulates the decision by the owner/operator to not address the vulnerability or the intent to resolve the vulnerability and a timeline for expected completion.
 - (3) Risk Acceptance. The decision by an owner/operator to accept a risk associated with an unresolved vulnerability should be made after careful consideration of the organization's risk tolerance, the potential impact if the risk becomes realized to the entity, individuals, geographic areas, other organizations, or society, and a cost-benefit analysis of the control measures that would be required to mitigate it.
 - (4) Submission of Amendments.

- (a) Additions of vulnerabilities to this Section do not necessarily require CSP amendment; the consolidated list of vulnerabilities should be treated as a living document given the dynamic nature of vulnerability management. The current version of the list is included in CSP submissions for initial approval, relevant amendment, or renewal.
 - (b) Changes to CSP provisions or impacts to the organization's security posture resulting from unresolved vulnerabilities and/or the incorporation of associated mitigations outlined in this Section should be considered by the owner/operator and any necessary amendments to the CSP submitted in accordance with 33 CFR 101.630(e).
- m. CSP Section 13 – Cyber incident reporting procedures in accordance with part 101 of this subchapter
Ref. 33 CFR 101.620(b)(7), 650(f)(2), 650(g)(1), Table 1
 - (1) Reporting. Procedures must be outlined for making required notifications to the Coast Guard and may include procedures for notifications to other entities/agencies. The owner/operator should designate who (by position and/or name) will be responsible for making notifications outside of the company and include contact information for the National Response Center and the cognizant COTP. NVIC 02-24 (series) provides guidance to harmonize the definitions of “cyber incident” under 33 CFR 6 and “reportable cyber incident” under 33 CFR 101 to streamline reporting while ensuring compliance with regulatory requirements. Procedures for reporting and recording any incident that falls under this harmonized definition must be documented. For specific guidance on incident reporting, see NVIC 02-24 (series).
 - (2) Supply Chain Incidents. As outlined in 33 CFR 101.650(f)(2), a process must be established and documented that requires IT and OT vendors/service providers to report to the owner/operator without delay the identification of any cybersecurity vulnerabilities or reportable cyber incidents.
 - (3) Cybersecurity threats.
 - (a) Cyber threats, as defined in 33 CFR 101.615, encompass malicious activities that may adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transit an information system. These threats may originate from external attackers or insider threats and may include events such as prewarning or unsuccessful phishing attacks or denial-of-service attacks or other unauthorized activities which attempt to exploit vulnerabilities or circumvent security measures in IT/OT systems.
 - (b) Entities must document cybersecurity threats in accordance with 33 CFR 101.640 and may source that information from actual incidents, vulnerability/security assessments including penetration tests, cybersecurity drills/exercises, and cyber threat intelligence. Cyber threats may present as suspicious activity, as defined in NVIC 02-24 (series). Entities are not required to document general information

about the multitude of cybersecurity threats and actors but rather should focus on actual threats and suspicious activity observed by the entity and/or specific threat groups/actors/tactics deemed a particular concern by the owner/operator.

n. CSP Section 14 – Cybersecurity Assessment (CSA)

Refs: 33 CFR 101.650(e)(1)-(2), Table 1

- (1) Many organizations will have assumptions, based on a clear and experience-based understanding of their environment, as to which systems are most essential and could potentially cause significant operational impacts or lead or contribute to a Transportation Security Incident (TSI) as defined in 33 CFR 101.100. Examples of such systems may include crane control systems, cargo-handling software, billing and metering systems, propulsion interfaces, safety automation and similar technologies.
- (2) A primary purpose of the CSA required under 33 CFR Part 101, Subpart F, is to validate those assumptions while also helping to identify additional, perhaps less obvious systems (for example, business, support, vendor, connectivity components etc.), that could introduce cybersecurity vulnerabilities or create operational risk pathways that may not have been evident upfront. Although the next to last step of the CSA process in this policy letter involves classifying assets as *Critical Information Technology (IT)* or *Operational Technology (OT)*, the regulatory mandates included in Subpart F are not limited to these systems. Instead, the regulation takes a more comprehensive approach to cybersecurity, with several baseline cybersecurity measures required for all IT/OT infrastructure of covered maritime entities. This guidance does not alter those requirements.
- (3) The initial cybersecurity assessment is the foundational first step in a continuous maturity process, not a final destination. A comprehensive assessment of the entire digital environment is critical; a narrow view can lead to wasted resources and leave unrecognized attack paths vulnerable. While a broad assessment may identify numerous issues, it does not obligate an entity to resolve every finding with major mitigation actions in the initial CSP. Instead, the CSA serves as the basis for aligning the owner/operator's risk management strategy with the requirements of reference (a). The owner/operator and the CySO use the CSA findings to develop the CSP. They must then annually validate that the CSP remains aligned with current threats, vulnerabilities, and the organization's risk tolerance. The Coast Guard expects that as an entity's cybersecurity program matures through regular updates, assessments, audits, drills, and exercises, it will continuously identify and address new or previously unrecognized risks.
- (4) Cybersecurity Officer Designation. The position of CySO ensures the regulated entity has a person with the necessary professional expertise to address cybersecurity. Properly scoping the CSA requires an understanding of cybersecurity equipment and systems, cybersecurity threats, best practices and methods for assessment. An entity that has not yet designated a CySO, nor has the requisite expertise on staff, may benefit from engaging that expertise and/or designating a CySO to oversee this process. The owner/operator is responsible for ensuring that the scoping and

assessment process is conducted by personnel with the requisite expertise or the ability to draw upon expert assistance to make informed findings on vulnerabilities and risks.

(5) Cybersecurity Assessment.

- (a) As defined in 33 CFR 101.615, the CSA is an appraisal of the risks facing an entity, asset, system, network, organizational operations, individuals, geographic areas, other organizations, or society and includes identification of relevant vulnerabilities and threats and determining the extent to which adverse circumstances or events could result in operational disruption and other harmful consequences.
- (b) As defined in 33 CFR 101.615, risk means a measure of the extent to which an entity is threatened by a potential circumstance or event and typically is a function of the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs and the likelihood of occurrence.
- (6) The “CSA Scoping and Process Guide” in Enclosure (4) is optional. Because the initial assessment forms the foundation of the CSP, it is highly consequential and should be rigorously conducted to identify vulnerabilities, threats, operational dependencies, and interdependencies that could result in operational disruption. Subsequent CSAs are required according to the schedule in §101.650(e)(1). These should be similarly rigorous as they serve to validate and update the CSP. This ensures the CSP remains current, effective, and aligned with evolving risks and operations. Because of the nature of cybersecurity threats and vulnerabilities, a complete cybersecurity assessment should involve both qualitative and technical assessment and cannot be effectively completed through only a visual check or cursory review.
- (7) CSAs for Waiver and Equivalency Determinations. An entity pursuing a Coast Guard approval for a waiver or equivalency request under any requirement of reference (a) is strongly recommended to utilize this guidance or another widely recognized industry standard to conduct and document the CSA to provide the necessary rigor of analysis and information to aid the Coast Guard in making a waiver or equivalency determination.
- (8) CSA Submission. As part of the CSP, the most current CSA must be submitted within Section 14 for plan approval and renewal. CSAs completed between renewal cycles should also be maintained in Section 14 and made available to the Coast Guard upon request.

3. GUIDE FOR CYBERSECURITY INCIDENT RESPONSE PLAN DEVELOPMENT

33 CFR 101.650(g)

- a. Purpose. This section provides optional guidance for the development, implementation, and evaluation of a Cybersecurity Incident Response Plan (CIRP) as defined in 33 CFR 101.615 and required in 33 CFR 101.650(g)(2).

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

- (1) The ultimate goals of cyber incident response are to recover the functional capabilities of an organization's systems, restore normal operations with minimal disruption to vital services and preserve business goals. For OT, IT and IoT systems and devices, emphasis in the CIRP should be placed on minimizing downtime, protecting vital processes, and mitigating risks that could impact physical safety, data integrity, or vital operations.
 - (2) While the priorities of an incident response may vary depending on an organization's unique operations, measures for recovering to a pre-incident state are inherent in an incident response plan and vital for resuming safe and secure operations of the MTS. CISA's Cybersecurity Performance Goals (CPGs) treat incident response and recovery as inseparable. Accordingly, the Coast Guard recommends that a CIRP encompass the full incident lifecycle, as customized to the owner/operator's unique operations and circumstances. Owners/operators are encouraged to ensure their CIRPs address not only how to contain and report a cyber incident but also how to restore vital systems, reestablish normal operations, and incorporate lessons learned.
- b. Process. The CIRP should describe the methods an entity will use to detect, respond, and recover from cybersecurity incidents that could adversely impact safe operations, security of the entity, or lead or contribute to a TSI. In aligning with broader business goals, the CIRP ensures that incident response efforts support operational continuity and stakeholder confidence. For example, entities with limited systems may rely mostly on contracted support for incident response, while entities with complex operations and systems may require multiple layers of responsibilities or playbooks. In all cases, the CIRP demonstrates an ability to coordinate and manage a cybersecurity incident scaled to the entity's size, complexity, and operational risk.



Figure 3 - Cyber Incident Response Lifecycle

- c. Pathway for Development. Regulated entities may find it useful to consult nationally and industry-recognized cybersecurity frameworks that provide common language and processes. These are not regulatory requirements, and entities may adopt alternative approaches. Options include, but are not limited to:
 - (1) NIST Cybersecurity Framework (CSF) 2.0: Outcome-based Functions, Categories, and Subcategories, which can be expressed as demonstrable capabilities.
 - (2) NIST SP 800-61r3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: Outlines best practices for creating, implementing, and improving incident response capabilities, focusing on effectively detecting, analyzing, mitigating, and recovering from cyber incidents.
 - (3) NIST SP 800-184, Guide for Cybersecurity Event Recovery: Provides organizations with best practices and strategies for effective cybersecurity event recovery, focusing on restoring systems, mitigating impact, and enhancing resilience to ensure operational continuity following a cyber incident.
 - (4) NISTIR 8428, Digital Forensics and Incident Response (DFIR) Framework for OT: Provides guidance on DFIR specifically tailored for addressing cybersecurity incidents in OT environments.
 - (5) NIST SP 800-82(series), Guide to OT Security: Provides comprehensive guidance on securing OT systems, offering best practices, risk management strategies, and recommendations to protect in ICS and other OT environments from cybersecurity threats.
- d. Plan Maintenance and Continuous Improvement. Although “Plan” appears in the title, the CIRP is not a regulatory plan in the same sense as a FSP, VSP, or CSP. Rather, it is a set of procedures that make up a required component of the CSP. Once established, the CIRP should be exercised regularly to validate effectiveness, with lessons learned promptly incorporated to ensure it remains current and relevant. The Coast Guard recommends the CIRP be treated as a “living document” that may be adjusted over time. The CIRP should be included in CSP audits, however, it is not expected or required that the CSP be amended or resubmitted to the Coast Guard when the CIRP is updated.
- e. Location. The Coast Guard recommends that the CIRP is kept as an Appendix to the CSP as noted in *Table 1*. If the CIRP is kept separate from the CSP, the location as well as details on implementation, maintenance, and exercise of the CIRP should be outlined in Sections 3 and/or 9 of the CSP.

4. ACRONYM LIST

AMS: Area Maritime Security
AMSC: Area Maritime Security Committee
ASP: Alternative Security Program
CFR: Code of Federal Regulations
CISA: Cybersecurity and Infrastructure Security Agency
CIRP: Cyber Incident Response Plan
COTP: Captain of the Port
CPG: Cybersecurity Performance Goal
CSA: Cybersecurity Assessment
CSF: Cybersecurity Framework
CySO: Cybersecurity Officer
DFIR: Digital Forensics and Incident Response
DHS: Department of Homeland Security
DoS: Denial of Service
EOL: End-of-Life
FSA: Facility Security Assessment
FSO: Facility Security Officer
FSP: Facility Security Plan
GPEN: GIAC Certified Penetration Tester
HMI: Human-Machine Interface
ICS: Industrial Control System
IDS: Intrusion Detection System
IIoT: Industrial Internet of Things
IPS: Intrusion Prevention System
ISAO: Information Sharing and Analysis Organization
ISAC: Information Sharing and Analysis Center
IT: Information Technology
KEV: Known Exploited Vulnerabilities
MAC: Media Access Control (address)
MDM: Mobile Device Management
MSC: Marine Safety Center
MTS: Marine Transportation System
MTSA: Maritime Transportation Security Act
NARA: National Archives and Records Administration
NEPA: National Environmental Policy Act
NIST: National Institute of Standards and Technology
NVIC: Navigation and Vessel Inspection Circular
OCMI: Officer in Charge, Marine Inspection

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-26
Enclosure (1) - Cybersecurity Plan Development and Maintenance Guidance

OCS: Outer Continental Shelf
OT: Operational Technology
PAC: Policy Advisory Council
PCI-DSS: Payment Card Industry Data Security Standard
PIV: Personal Identity Verification
POAM: Plan of Actions and Milestones
RTO: Recovery Time Objective
RPO: Recovery Point Objective
ROE: Rules of Engagement
SCADA: Supervisory Control and Data Acquisition
SCRM: Supply Chain Risk Management
SLR: Service Level Requirement
SOC: Security Operations Center
SP: Special Publication
SI: Super Intelligence (formerly known as Artificial Intelligence)
SSI: Sensitive Security Information
TSI: Transportation Security Incident
TWIC: Transportation Worker Identification Credential
USCG: United States Coast Guard
USC: United States Code
VSA: Vessel Security Assessment
VSO: Vessel Security Officer
VSP: Vessel Security Plan

Enclosure (2)
Sample CySO Designation Letter

Company Letterhead

Cyber Security Officer (CySO)/ Alternate Cyber Security Officer (ACySO) Designation

Name of Designee: _____

CySO / ACySO (circle one) for (MTSA Facility/Vessel/OCS Facility name and address):

Affiliation

{Select one.}

☐ Employee.

☐ Support Contractor. If support contractor, provide name and contact information of contracting company:

Designating Official

{Owner/Operator}

Name: _____ Title: _____

Signature: _____ Date: _____

Review and Approval

{e.g., Chief Information Officer}

Name: _____ Title: _____

Signature: _____ Date: _____

Comments:

Notice

This enclosure represents optional information that may be included in a CySO Designation Letter. Owners/operators may use a different format so long as the CySO is clearly designated, meets the regulatory requirements under 33 CFR 101.625(e), and is aware of their responsibilities under 33 CFR 101.625(d). This example lists those requirements, but need not necessarily be included in a designation letter.

CySO / ACySO Acknowledgment of Responsibilities

I, _____ (full name), have been formally designated a/an:

☐ Cyber Security Officer (CySO) or ☐ Alternate Cyber Security Officer (ACySO)

for _____ [Facility, Vessel, or OCS Facility Name], and I understand that my responsibilities according to Title 33, Code of Federal Regulations, Part 101 Subpart F are listed below. I must:

- Ensure that the Cybersecurity Assessment is conducted as required by this part.
- Ensure the cybersecurity measures in the Cybersecurity Plan are developed, implemented, and operating as intended.
- Ensure that an annual audit of the Cybersecurity Plan and its implementation is conducted and, if necessary, ensure that the Cybersecurity Plan is updated.
- Ensure the Cyber Incident Response Plan is executed and exercised.
- Ensure the Cybersecurity Plan is exercised in accordance with [§ 101.635\(c\)](#)
- Arrange for cybersecurity inspections, which may be conducted as their own inspections, or in conjunction with any scheduled Coast Guard inspection of a U.S.-flagged vessel, facility, or OCS facility.
- Ensure the prompt correction of problems identified by exercises, audits, or inspections.
- Enhance the cybersecurity awareness and vigilance of personnel.
- Ensure adequate cybersecurity training of personnel.
- Ensure all reportable cyber incidents are recorded and reported to the owner/operator.
- Ensure that records required by this part are maintained in accordance with [§ 101.640](#).
- Ensure any reports as required by this part have been prepared and submitted.
- Ensure that the Cybersecurity Plan, as well as proposed amendments to cybersecurity measures, are submitted for approval to the cognizant COTP or the Officer in Charge, Marine Inspections (OCMI) for facilities or OCS facilities, or to the Office of Maritime Cybersecurity Policy (CG-MCP) for U.S.-flagged vessels, prior to amending the Cybersecurity Plan, in accordance with [§ 101.630](#).
- Ensure relevant security and management personnel are briefed regarding changes in cybersecurity conditions on board the U.S.-flagged vessel, facility, or OCS facility.
- Ensure identification and mitigation of all KEVs in critical IT or OT systems, without delay.
- Additional requirements from owner/operator _____

Qualifications

I have general knowledge, through training, education, or equivalent job experience, in the following:

- General vessel, facility, or OCS facility operations and conditions;
- General cybersecurity guidance and best practices;
- The vessel, facility, or OCS facility's Cyber Incident Response Plan;
- The vessel, facility, or OCS facility's Cybersecurity Plan;
- Cybersecurity equipment and systems;
- Methods of conducting cybersecurity audits, inspections, control, and monitoring techniques;
- Relevant laws and regulations pertaining to cybersecurity;
- Instruction techniques for cybersecurity training and education;
- Handling of Sensitive Security Information and security-related communications;
- Current cybersecurity threat patterns and KEVs;
- Recognizing characteristics and behavioral patterns of persons who are likely to threaten security;
- Conducting and assessing cybersecurity drills and exercises; and,
- Any additional requirements from owner/operator as specified:

I hereby certify that I have read, understood and agree to the responsibilities of this position, and I certify that I meet or exceed the qualifications listed above.

Signature: _____

Date: _____

Job Title: _____

Phone Number: _____

Enclosure (3)
Penetration Testing Guidance

Penetration Testing Guidance

1. Discussion. Penetration testing represents a crucial element of a comprehensive cybersecurity strategy in the quickly evolving landscape of cyber threats. In accordance with 33 CFR 101.615, a penetration test means a test of the security of a computer system or software application by attempting to compromise its security and the security of an underlying operating system and network component configurations. A penetration test should simulate realistic attack scenarios under tightly controlled and pre-agreed conditions. It involves proactively testing computer systems, networks, and software applications to identify vulnerabilities that might be exploited by attackers. Penetration testing supplements other cybersecurity risk measures in the regulations such as annual CSAs, vulnerability scans, and routine system maintenance.
2. Scope. The Coast Guard recognizes that active vulnerability scanning and penetration testing on some live OT and industrial control systems may present unacceptable risks to physical safety, vessel navigation, and facility operations. In these cases, the owner/operator should consider penetration testing of the OT boundary, weigh the risk of OT inclusion, and determine the scope of the penetration test based on the CSA and operational risk. It is the owner/operator's responsibility to determine an appropriate scope for penetration testing across both IT and OT environments that effectively tests the entity's cybersecurity posture based on the scope, findings, and risks identified in the CSA. The owner/operator should consider not only critical IT and OT systems, but also networks and connections that could allow for lateral movement and potential compromise of critical systems or otherwise negatively impact operations.
3. Process. The objective is to evaluate the effectiveness of existing security measures and identify exploitable vulnerabilities.
 - a. Phases. Phases of a complete penetration test typically include:
 - (1) *Phase 1 - Planning*. Sets the groundwork with no actual testing being done. Establishes the Rules of Engagement (ROE) and ensures all parties agree with what systems and methods the penetration testing will include.
 - (2) *Phase 2 - Discovery*. Includes gathering information on the network such as identifying network ports and services to determine potential targets.
 - (3) *Phase 3 - Attack*. Executing the attack is at the heart of any penetration test. If an attack is successful, the vulnerability being exploited is verified and mitigations can be determined to improve the associated security posture. If not successful, the attack may instead result in learning more about the targeted network and its potential vulnerabilities.
 - (4) *Phase 4 - Reporting*. Occurs simultaneously with the other three phases. At the conclusion of the penetration test, a report should be generated by the assessor that describes identified vulnerabilities, presents a risk rating, and recommends mitigations.
 - b. Penetration Tester Qualifications. The Coast Guard will not recommend any specific penetration testing provider. The selection of a penetration testing provider should be informed by and customized to the entity's operational needs and security risk. If the entity does not have technical expertise, then an external provider must conduct the penetration testing. Considerations for the owner/operator when selecting a penetration tester include:

- (1) Familiarity with maritime IT, OT and industrial control systems;
 - (2) Understanding of the operational context, regulatory requirement and safety constraints;
 - (3) Demonstrated ability to plan and conduct tests under Rules of Engagement (ROE);
 - (4) Certifications (e.g., GPEN, CEH, PenTest+) may assist in verifying skill sets but do not replace sound governance or risk-informed planning.
- c. Penetration Test Frequency. Penetration testing is required at least once every CSP renewal cycle, aligning the test frequency with the CSP's approval process. This ensures vulnerabilities are assessed and validated on a recurring basis without prescribing a fixed calendar interval. Penetration testing must occur any time between approval of the CSP and submission of the next CSP on a five-year cycle, with the recommendation being within 24 months before CSP renewal to inform the update of the CSP. Penetration testing is not required for the initial submission due in July 2027. Further guidance regarding penetration testing is currently under development and will be issued at a later date.

Enclosure (4)

Cybersecurity Assessment (CSA) Scoping and Process Guidance

Cybersecurity Assessment (CSA) Scoping and Process Guidance

1. The regulations require a CSA to “analyze all networks to identify vulnerabilities to critical IT and OT and the risk posed by each digital asset” in 33 CFR 101.650(e)(1)(i). An effective way to interpret this mandate is as a risk-filtering process. First, inventory all systems, dependencies, and interfaces, not just those individual systems that obviously meet the definition of critical IT and OT. An illustrative example of asset categorization discovered during inventory is provided in *Figure 4*.
2. The owner/operator’s responsibility to address cybersecurity risk to maritime operations is different than implementing physical security measures such as gates, guards, and fences. Owners/operators have the choice to locate/host/subscribe to IT, OT, and cybersecurity systems onsite at a regulated entity, in the cloud, or remotely anywhere in the world. Regardless of where entity systems are located, they may still pose risk to the maritime operations of the regulated entity. Accordingly, the CSA should address any systems and functions that could lead to a cyber incident, operational disruption or TSI at the maritime entity. Such risks must be addressed in the CSP under 33 CFR 101.630.

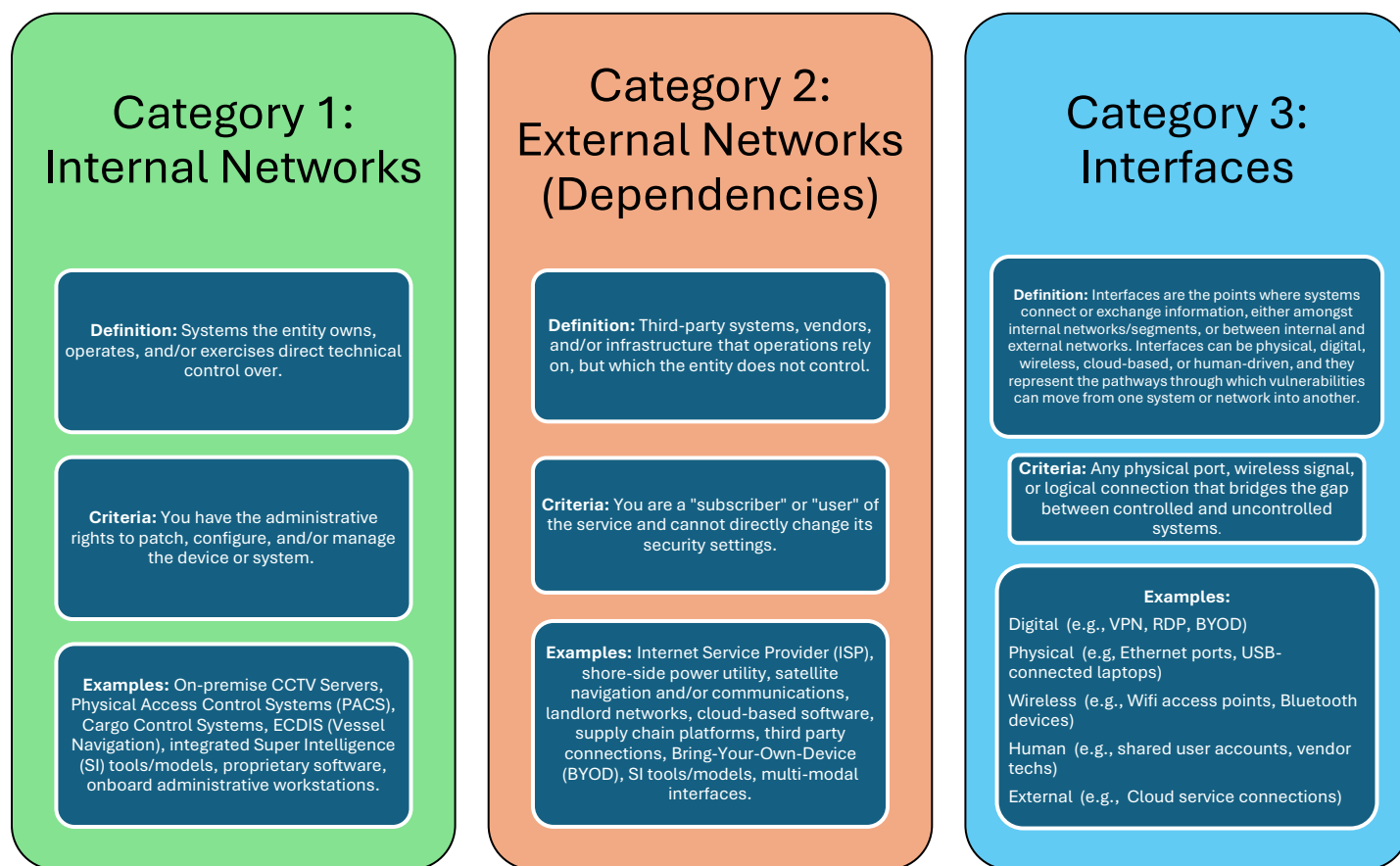


Figure 4 - Categorization of Network Assets and Systems¹

3. The Coast Guard does not regulate contractor or third-party entity networks (Category 2); however, the owner/operator is responsible for the entity’s risk management processes for dependence on those external services. If an external network, service, or system can lead to a cyber incident,

¹ Artificial Intelligence (AI) has been redesignated as Super Intelligence (SI) in accordance with Executive Order 14434 of September 29, 2026, “Inaugurating the Era of Super Intelligence.”

operational disruption, or TSI at the maritime entity, the CSA should analyze those dependencies.

4. A visualization of the CSA risk-filtering process is provided in *Figure 5*, based on the process in *Table 8*. *Table 8* provides an optional guide for conducting a CSA and identifying critical IT/OT. Although NIST standards² are referenced in this document, entities are free to utilize other industry standards or assessment frameworks/models to conduct a CSA with equivalent or greater rigor, and entities should identify the standard(s) used in the CSA report.
5. The NIST Cybersecurity Framework (CSF) and supporting NIST documents are referenced in this process to demonstrate the grounding of the CSA guide in current accepted practice and to provide avenues for consistent additional information, if needed, that aligns with the CSA guide's approach. The NIST CSF helps manage and reduce cybersecurity risks with a grouping of high-level outcomes that any organization can scale and use to understand, assess, prioritize, and communicate its cybersecurity efforts. It also links to resources that provide additional guidance on practices and controls for achieving security outcomes. The NIST CSF allows entities to use their preferred methods for control selection.
6. Although NIST standards are referenced in this document, entities are free to utilize other industry standards or assessment frameworks/models to conduct a CSA with equivalent or greater rigor, and entities should identify the standard(s) used in the CSA report. For small/medium businesses not currently using NIST CSF but interested in doing so, NIST has created a [Small Business Cybersecurity Corner](#) with various quick start guides, references, videos, and training tailored to small business needs.

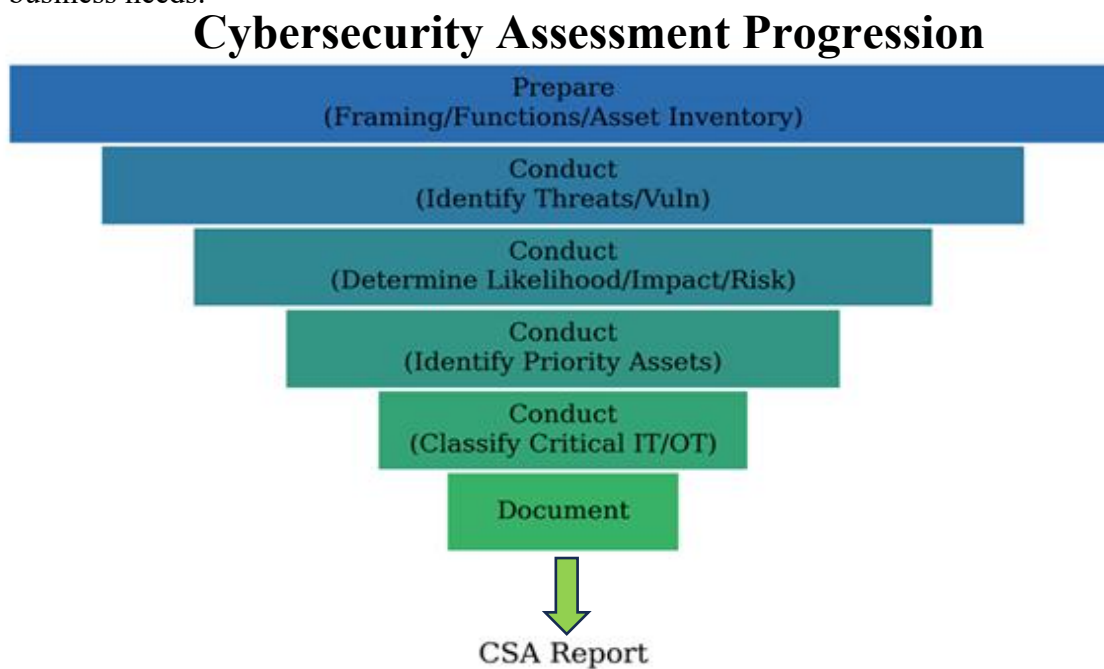


Figure 5 - CSA Risk Filtering Process

² The NIST documents referenced in the development of this guide were:

- a. NIST Cybersecurity Framework
- b. NIST SP 800-30 (Series) Chapter 3 & Appendix D – I
- c. NIST SP 800-53
- d. NIST IR 8286A-D (Series)
- e. NIST SP 800-37 (Series)

Stage	Description	Action
1. PREPARE a. Framing the CSA	Process whereby the organization establishes a common perspective, intent, and strategy for how they will conduct the CSA.	Ensure shared understanding amongst CySO, owners/operators, senior leaders, and any individuals/team members designated to conduct the CSA regarding risk management concepts and the intent and scope of the assessment. Determine <i>Risk Tolerance</i> – level of risk the organization is willing to accept to achieve its operational or business objectives. Identify <i>Assumptions</i> – things the organization presumes to be true at the outset of the CSA, even if not yet verified (e.g., All primary OT systems are effectively segmented). Identify <i>Constraints</i> – limitations that may restrict the scope, timeframe, depth, or methodology of the CSA (e.g., resources, technical, access, and operational).
1. PREPARE b. Determine Necessary Functions	The foundational activity of creating a comprehensive master list of all operational, business, administrative, and support functions that are necessary for the entity to operate or deliver goods or services.	Entities should identify the functions and business processes that are essential for successful operations. The loss, interruption, or impairment of these functions or processes may have negative implications for safety, security, or the entity’s ability to meet its business objectives.
1. PREPARE c. Inventory and Categorize Assets	The foundational activity of developing a comprehensive asset inventory, as required in 33 CFR 101.650(b)(3) to facilitate a detailed analysis of “all networks” as mandated in 33 CFR 101.650(e)(1)(i).	Various methods may be employed including system discovery, network mapping, and staff interviews to thoroughly catalogue all assets (see <i>Note 1</i>). Each asset should be categorized as Internal, External (Dependency), or Interface as described in <i>Figure 4</i>.

Stage	Description	Action
2. CONDUCT <i>a. Identify Threats</i> <i>b. Identify Vulnerabilities</i> <i>c. Determine Likelihood</i> <i>d. Determine Impact</i> <i>e. Determine Risk</i>	The process of determining the risk posed by each inventoried asset through an analysis of relevant threats, vulnerabilities, the likelihood of compromise, and the potential impact from successful exploitation. Ensure objective evaluation of all systems to prevent premature assumptions of ‘no risk’.	Identify threat sources relevant to the entity and threat events that could be produced by those sources. Identify vulnerabilities (technical and/or procedural) of the entity’s inventoried assets (1.c) that could be exploited by threat sources (see <i>Note 2</i>). Determine the likelihood that identified threat sources would initiate a threat event against inventoried assets and the likelihood of their success. Determine the adverse impacts to operations, assets, individuals, other critical infrastructure, and the community, from the successful exploitation of vulnerabilities. Determine risk associated with each inventoried asset as a combination of the likelihood of threat exploitation of vulnerabilities and the impact of such exploitation. The thresholds outlined under the definition of ‘reportable cyber incident’ in 33 CFR 101.615 may be informative in this process to entities without established business risk thresholds.
2. CONDUCT <i>f. Identify Priority Assets</i>	A process informed by the completed risk analysis of each inventoried IT/OT asset to identify those assets that connect to or have a role in facilitating the organization’s necessary functions/processes.	Identify which systems on the asset inventory (1.c) directly perform, support or enable the master list necessary functions/processes (1.b). These priority assets also include systems on the asset inventory that do not directly perform, support, or enable a master list necessary function/process but are connected, either physically or logically, to systems that do.

Stage	Description	Action
2. CONDUCT <i>g. Critical IT/OT Classification</i>	Process of determining, based on the completed risk analysis, which priority assets must be designated as Critical IT and OT systems as defined in 33 CFR 101.615. Systems designated as Critical IT or OT are subject to specific security measures mandated within 33 CFR 101.650.	Consider the risk and potential impact associated with each priority asset and determine whether a substantial loss or degradation of confidentiality, integrity, or availability of that system could result in a Transportation Security Incident (TSI) as defined in 33 CFR 101.105. If the answer is “Yes” or “Maybe” (see <i>Note 3</i>), the asset should be designated as Critical IT/OT by the CySO or owner/operator if a CySO has not yet been designated. Designated Critical IT/OT should be the focus of in-depth vulnerability (and Known Exploited Vulnerability) identification and mitigating/ compensating controls.
3. COMMUNICATE & DOCUMENT <i>a. Share Information</i> <i>b. Document Results, Recommendations, and Resolutions</i>	Process of communicating risk assessment results to entity decision makers to support risk responses and documenting vulnerabilities to Critical IT/OT and the risk posed by each digital asset.	Document vulnerabilities, recommendations and resolutions in the CSA Report which will be maintained with the Cybersecurity Plan. Ensure the CSA Report is marked, handled, stored and transmitted as Security Sensitive Information (SSI) under 49 CFR 1520.

Table 8 - CSA Process Guide

Note 1: *The inventory and/or the map should include these categories:*

- 1. OT device configuration information (33 CFR 101.650(b)(4));*
- 2. After completion of CSA, denote identified critical IT/OT systems (33 CFR 101.650(b)(3)).*

As determined by the owner/operator, customized additional categories for each device may include, but are not limited to:

- 1. System Name and Unique Identifier*
- 2. Location (physical and logical) (33 CFR 101.650(i))*
- 3. Operating System and Version*

4. *Hardware Specifications such as device type, manufacturer, model, MAC Address, IP address (if fixed)*
5. *OT device configuration, including any OT connected to publicly accessible internet with justification (33 CFR 101.650(b)(4),(e)(3)(v))*
6. *OT-related IT (33 CFR 101.650(i)(1))*
7. *Software Applications, Versions, and License Information*
8. *Owner/Custodian*
9. *Purpose/Function*
10. *Last Patch/Update Date (33 CFR 101.650(e)(3)(i))*
11. *Risk-based prioritization of assets (filled out after CSA completion)*
12. *Dependencies and Interconnections with other systems*
13. *Maintenance Status and History*
14. *Applications with executable code disabled by default and those with executable code still running on critical IT/OT (33 CFR 101.650(b)(2)).*

Note 2: *Vulnerability identification methods used should align with the entity's risk exposure and risk tolerance, operational complexity, and governance approach. Vulnerabilities may be technical or procedural and identified through a combination of patch and configuration reviews, system/network scanning, architecture reviews, and/or operational and procedural analysis.*

Note 3: *“Yes” and “No” determinations may be straightforward. However, “Maybe” determinations necessitate additional scrutiny when determining Critical IT/OT. Depending on the entity's specific operating conditions, examples of possible “Maybe” systems/devices and considerations include, but are not limited to:*

1. *Fuel monitoring or tank level sensors may not control equipment directly, but manipulated data could delay detection of unsafe conditions.*
2. *A badge access management system computer may appear administrative, yet compromise could enable unauthorized entry into restricted or secure areas.*
3. *A cargo billing or release system may not control physical operations, but if compromised could halt cargo movement and create cascading operational disruption.*