U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

US Coast Guard
Mail Stop 7501
Washington, DC 20593-7501
Staff Symbol: CG-5P
Phone: (202) 372-1111

16000
CG-5PC Policy Letter 01-26
June 2, 2026

From: Robert C. Compher, CAPT
COMDT (CG-5PC)

To: Distribution

Subj: CYBERSECURITY ASSESSMENT INITIAL SCOPING AND PROCESS

Ref: (a) Title 33, Code of Federal Regulations, Subchapter H (Maritime Security)
(b) Navigation and Vessel Inspection Circular (NVIC) 02-24, CH 1

1. Purpose. This policy letter provides guidance for determining the scope of the Cybersecurity Assessment (CSA) required under 33 CFR 101.650. The outcomes and findings of the CSA inform the development of the Cybersecurity Plan (CSP). The purpose of this guidance is to ensure consistent national implementation across the Marine Transportation System (MTS) and to assist owners, operators, and Cybersecurity Officers (CySOs) in defining this scope to ensure resources are focused on risks they can impact, while planning for other risks they cannot.

2. Applicability. This policy letter applies to all U.S.-flagged vessels, facilities, and OCS facilities required to have a security plan under 33 CFR 104, 105, and 106. In this guidance, this group, which also includes the owners, operators, and CySOs, will collectively be referred to as "entities" for brevity but does not change the specific responsibility designations in Reference (a). If guidance specifically applies to a subset of this group, it will be individually identified. This policy letter will be distributed by electronic means only. It is available at the USCG Maritime Industry Cybersecurity Resource Website.

3. Discussion.

   a. 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 result in 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.

   b. A primary purpose of the Cybersecurity Assessment (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 <u>all</u> IT/OT infrastructure of maritime entities[1]. This policy letter does not alter those requirements.**

c. 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 Cybersecurity Plan (CSP). Instead, the Cybersecurity Assessment (CSA) serves as the basis for aligning the owner/operator's risk management strategy with the requirements of 33 CFR 101 Subpart F. The owner/operator and the Cybersecurity Officer (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. <u>Cybersecurity Officer Designation</u>. 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, will 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. <u>CSA Assessment Process</u>.

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.

c. Required elements for a CSA are detailed in 33 CFR 101.615 and 33 CFR 101.650 (e)(1). Enclosure (1) contains an **optional** guide to conducting a CSA. Because it forms the foundation of the CSP, the initial assessment is highly consequential and should be

[1] These requirements are detailed in 33 CFR 101.650 (a-c, e-f, h-i).

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.

6. CSAs for Waiver and Equivalency Determinations. An entity pursuing a Coast Guard approval for a waiver or equivalency request (under any requirement of 33 CFR 101 Subpart F) is strongly recommended to utilize this guidance or another widely recognized industry standard method 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.

7. Disclaimer. This policy is not a substitute for applicable legal requirements, nor is itself a rule. It provides operational guidance for U.S. Coast Guard personnel and the maritime industry. It does not impose legally binding requirements on any party outside of the U.S. Coast Guard. The regulatory requirements in reference (a) remain in effect and are unchanged by this policy.

8. Questions concerning this policy should be directed to MTSCyberRule@uscg.mil.

#

CSA Scoping and Process Guide

1. A CSA is required to "analyze all networks to identify vulnerabilities to critical IT and OT and the risk posed by each digital asset" under 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/OT. An illustrative example of categorization of assets discovered during the inventory is provided in *Figure 1*.

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 account for 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.

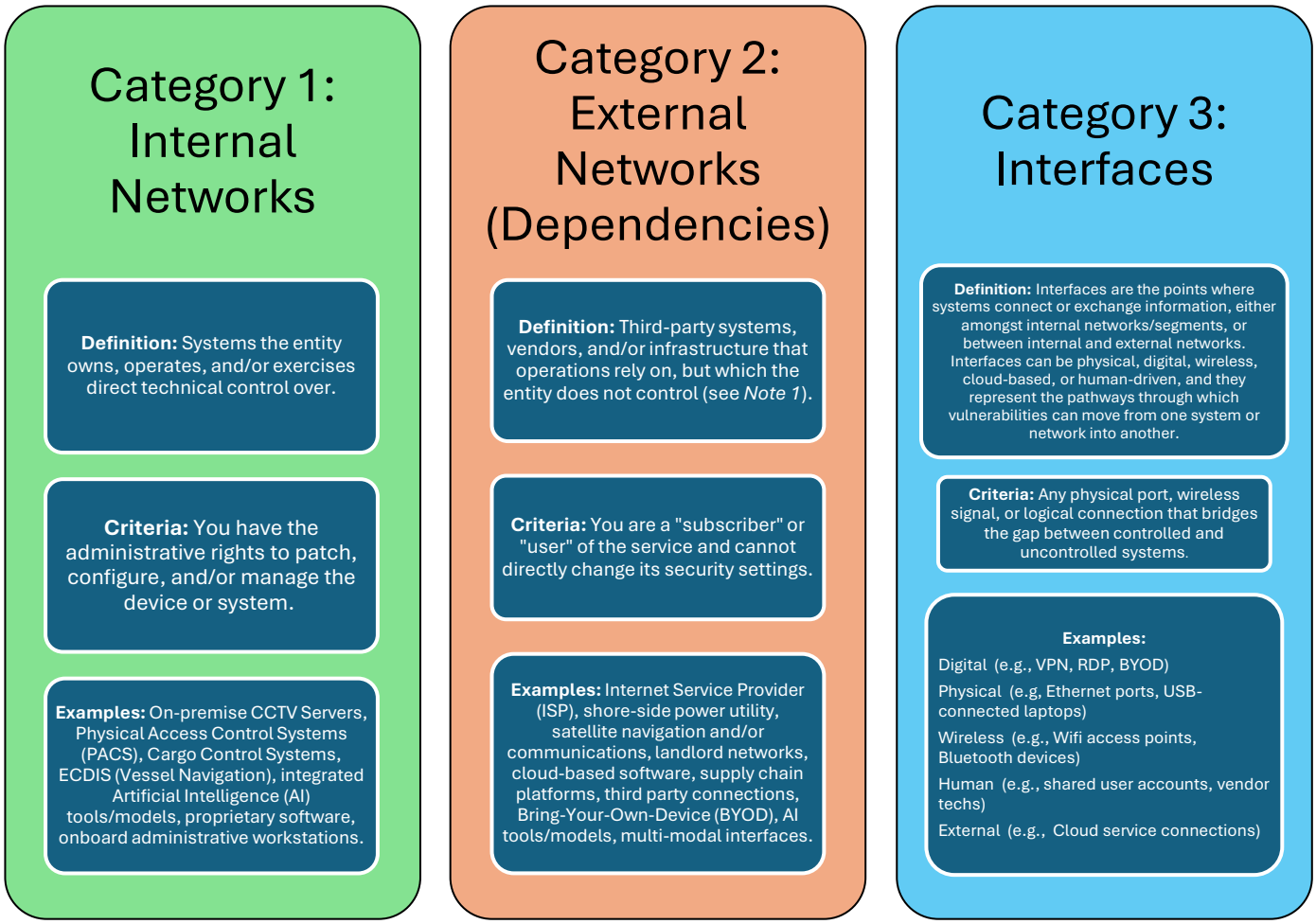


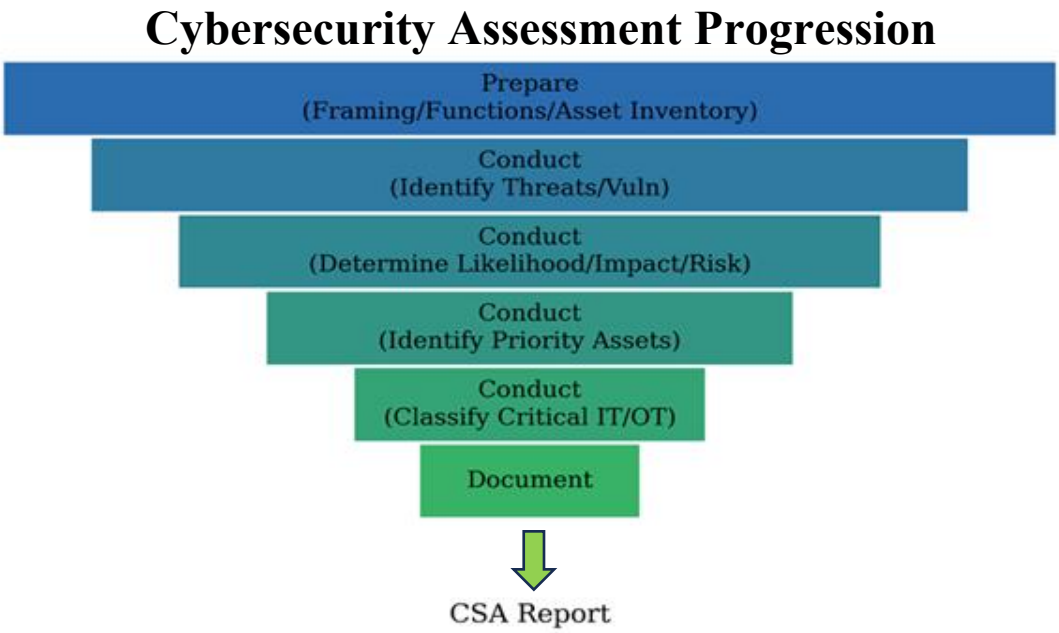
Figure 1 - Categorization of network assets and systems

3. The Coast Guard does not regulate contractor or third-party entity networks; however, the owner/operator is responsible for the regulated entity's risk management processes for dependence

on those external services. If an external network, service, or system can lead to a cyber incident, 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 2*, based on the process in *Figure 3*. *Figure 3* provides an optional guide for conducting a CSA and identifying critical IT/OT. Although NIST standards[2] 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. 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.



[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 (Series)
e. NIST IR 8286B (Series)
f. NIST IR 8286C (Series)
g. NIST IR 8286D (Series) Section 2
h. NIST SP 800-37 (Series)

Figure 2 - CSA Risk Filtering Process

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, owner/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 *Risk Tolerance* – level of risk the organization is willing to accept to achieve its operational or business objectives. Identify *Assumptions* – 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 *Constraints* – 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 *Note 1*). Each asset should be categorized as **Internal**, **External** (Dependency), or **Interface** as described in *Figure 1*.

Stage	Description	Action
2. CONDUCT ***a. Identify Threats*** ***b. Identify Vulnerabilities*** ***c. Determine Likelihood*** ***d. Determine Impact*** ***e. Determine Risk***	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 *Note 2*). 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 ***f. Identify Priority Assets***	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 ***g. Critical IT/OT Classification***	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" (for context, see *Note 3)*, 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 ***a. Share Information*** ***b. Document Results, Recommendations and Resolutions***	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.

Figure 3. 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 must 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 whether or not they should be included as 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.*