

Third-Party Vendor Cybersecurity Compliance Certification Form
(Aligned with 33 CFR 101.650 – Maritime Cybersecurity Measures)

Vendor Information Vendor Company Name: _____

Address: _____

Primary Contact: _____

Phone: _____ Email: _____

Date of Certification: _____

Services/Products Provided (brief description, e.g., IT/OT systems, cloud services, network management, software for critical operations):

Certification Statement

The undersigned, on behalf of the Vendor named above, hereby certifies that, to the best of our knowledge and based on reasonable due diligence, the services, products, and/or systems provided to [Your Company/Facility/Vessel Name] comply with applicable cybersecurity requirements, including those considerations outlined in 33 CFR 101.650 (Cybersecurity measures) under the U.S. Coast Guard's Maritime Security regulations.

Specifically, the Vendor confirms implementation of the following key measures (check all that apply or provide explanation where not fully applicable):

#	Cybersecurity Measure (per 33 CFR 101.650)	Compliant (Yes/No/Partial)	Comments/Evidence (e.g., policies, certifications, controls in place)
1	Account security measures (e.g., multi-factor authentication, unique accounts, least privilege)		
2	Device security measures (e.g., endpoint protection, secure configuration, inventory)		
3	Network security and segmentation (e.g., firewalls, segmentation of IT/OT networks)		
4	Data security and encryption (e.g., protection of data at rest and in transit)		
5	Cybersecurity training for relevant personnel		

# Cybersecurity Measure (per 33 CFR 101.650)	Compliant (Yes/No/Partial)	Comments/Evidence (e.g., policies, certifications, controls in place)
6 Risk management, including vulnerability identification, scanning, and timely patching of Known Exploited Vulnerabilities (KEVs)		
7 Penetration testing and cybersecurity assessment (as applicable)		
8 Incident response and recovery planning (including reporting of reportable cyber incidents)		
9 Supply chain/third-party risk management (for any sub-vendors used)		
10 Logging, monitoring, and resilience measures		

Additional Attestations

- The Vendor maintains a Cybersecurity Plan or equivalent program addressing the above measures.
- The Vendor agrees to notify [Your Company] without delay of any reportable cyber incident affecting provided services/systems.
- The Vendor permits reasonable audits, assessments, or information requests related to cybersecurity compliance upon request.
- Supporting documentation (e.g., SOC 2 report, ISO 27001 certification, NIST alignment statement) is available upon request: Yes / No (list if applicable): _____

Declaration I certify that the information provided in this form is true, accurate, and complete. The Vendor understands that false statements may result in termination of services and potential regulatory consequences.

Signed: _____ Date: _____ Name: _____
 _____ Title: _____

For Recipient Use Only ([Your Company/Facility/Vessel]) Reviewed by:

_____ Date: _____ Approved: Yes / No

Notes: _____