USCG CYBER INSPECTION

VESSEL IMO: _____ **DATE:_____**

Please check each item and provide any relevant notes.

1. NC – Network Connectivity

Question	Yes	No	If YES → Follow-Up (mark Yes/No)	If NO → Follow-Up (mark Yes/No)
Does the vessel connect to external networks through secure channels (e.g., VPN, MFA)?			Are VPN/MFA logs reviewed regularly? Yes ☐ / No ☐ Are connections audited for vulnerabilities? Yes ☐ / No ☐ Are all devices using approved encryption? (AES) Yes ☐ / No ☐ Are crew trained annually on secure network use? Yes ☐ / No ☐	What type of connection is used documented? Yes ☐ / No ☐ Is access restricted by IP/device/user role? Yes ☐ / No ☐ Are crew trained on insecure network risks? Yes ☐ / No ☐ Is MFA used for any services? Yes ☐ / No ☐
Are operational and recreational networks segmented or firewalled?			Are firewall rules updated after changes? Yes ☐ / No ☐ Are segmentation tests done in drills? Yes ☐ / No ☐	Are both networks on the same switch/router? Yes ☐ / No ☐ Any incidents linked to lack of separation? Yes ☐ / No ☐ Are firewalls installed between systems? Yes ☐ / No ☐ Is internet browsing allowed on OT system? Yes ☐ / No ☐
Do onboard systems interface with shore-based systems?			Are secure transfer protocols used? Yes ☐ / No ☐ Are shore systems vetted for compliance? Yes ☐ / No ☐ Are transfer logs reviewed after each session? Yes ☐ / No ☐	Are secure transfer protocols unavailable? Yes ☐ / No ☐ Are shore-based systems audited? Yes ☐ / No ☐

USCG CYBER INSPECTION

2. UP – System Updates & Maintenance

Question	Yes	No	If YES → Follow-Up (mark Yes/No)	If NO → Follow-Up (mark Yes/No)
Are system patches and updates applied regularly?			Is the patching schedule documented in the FSP? Yes ☐ / No Are patches tested before deployment? Yes ☐ / No ☐ Are post-patch vulnerability scans conducted? Yes ☐ / No ☐	When were critical systems last patched? Yes ☐ / No ☐ Who is responsible (ship or shoreside)? Yes ☐ / No ☐ Is there vulnerability tracking? Yes ☐ / No ☐ Contingency plan for unpatched vulnerabilities? Yes ☐ / No ☐
Are navigational charts updated and verified for accuracy?			Are update logs reviewed & signed by the officer responsible? Yes ☐ / No ☐ Are chart updates tested in ECDIS simulations? Yes ☐ / No ☐	Who is responsible for verification? Yes ☐ / No ☐ When were charts last updated? Yes ☐ / No ☐
Is antivirus software installed and maintained onboard?			Are definitions updated automatically? Yes ☐ / No ☐ Are update logs retained and checked? Yes ☐ / No ☐ Are bridge systems scanned weekly? Yes ☐ / No ☐	Are endpoints protected? Yes ☐ / No ☐ Are USB ports disabled/controlled? Yes ☐ / No ☐ Past malware infections? Yes ☐ / No ☐ What compensating controls exist? Yes ☐ / No ☐

USCG CYBER INSPECTION

3. AC – Access Control

Question	Yes	No	If YES → Follow-Up (mark Yes/No)	If NO → Follow-Up (mark Yes/No)
Are remote access activities logged and reviewed regularly?			Are access logs stored securely and protected from alteration? Yes ☐ / No ☐ Are remote access privileges reviewed during crew changes? Yes ☐ / No ☐ Are cyber & physical security teams coordinating anomalies? Yes ☐ / No ☐	Is remote access used at all? Yes ☐ / No ☐ Who can remotely connect? Yes ☐ / No ☐ How are unauthorized logins detected? Yes ☐ / No ☐ Any backup access review policy? Yes ☐ / No ☐
Have there been signs of unauthorized access or suspicious login attempts?			Was the incident documented and reported? Yes ☐ / No ☐ Were passwords changed after? Yes ☐ / No ☐ Was it linked to an external IP? Yes ☐ / No ☐ What corrective measures were implemented? Yes ☐ / No ☐	Is monitoring in place to detect attempts? Yes ☐ / No ☐ Are alarms or alerts configured? Yes ☐ / No ☐

4. AT – Cyber Threats & Attacks

Question	Yes	No	If YES → Follow-Up (mark Yes/No)	If NO → Follow-Up (mark Yes/No)
Have any phishing or social engineering attempts been reported?			Were incidents reported to the Coast Guard? Yes ☐ / No ☐ Were corrective measures documented in FSP? Yes ☐ / No ☐ ☐ Was additional crew training conducted afterward? Yes ☐ / No ☐	Are crew trained to identify phishing? Yes ☐ / No ☐ Are suspicious emails quarantined automatically? Yes ☐ / No ☐ Is there an onboard contact to report attempts? Yes ☐ / No ☐
Have there been any recent threat alerts or cybersecurity incidents?			Was a risk assessment or drill conducted after the incident? Yes ☐ / No ☐ Were lessons learned shared with crew/company? Yes ☐ / No ☐	Has the company issued cyber bulletins in last 6 months? Yes ☐ / No ☐ Are vessel systems monitored for anomalies? Yes ☐ / No ☐ Has a formal risk assessment been done? Yes ☐ / No ☐

USCG CYBER INSPECTION

5. SB – System Behavior & Stability

Question	Yes	No	If YES → Follow-Up (mark Yes/No)	If NO → Follow-Up (mark Yes/No)
Have there been system failures or abnormal behavior recently?			Were anomalies logged and analyzed in FSA? Yes ☐ / No ☐ Were mitigation steps tested afterward? Yes ☐ / No ☐	Are logs kept of system health? Yes ☐ / No ☐ Any suspicion of concealment? Yes ☐ / No ☐
Has the vessel experienced GPS spoofing or AIS anomalies?			Were anomalies reported to authorities? Yes ☐ / No ☐ What mitigation steps were taken? Yes ☐ / No ☐ Were drills conducted to simulate similar attacks? Yes ☐ / No ☐	N/A

6. CSC – Cybersecurity Systems & Controls

Question	Yes	No	If YES → Follow-Up (mark Yes/No)	If NO → Follow-Up (mark Yes/No)
Is there a recreational computer isolated from operational networks?			Are isolated systems scanned for malware before crew use? Yes ☐ / No ☐ Are USB transfer logs reviewed? Yes ☐ / No ☐	Can crew access the internet on shared systems? Yes ☐ / No ☐ Any virus transfers from USBs/laptops? Yes ☐ / No ☐
Are up-to-date IT/OT infrastructure diagrams available onboard?			Are diagrams reviewed after hardware/software changes? Yes ☐ / No ☐ Are changes logged in FSP? Yes ☐ / No ☐	Who maintains system diagrams? Yes ☐ / No ☐ When were diagrams last reviewed? Yes ☐ / No ☐

USCG CYBER INSPECTION

7. CC – Company Communication History

Question	Yes	No	If YES → Follow-Up (mark Yes/No)	If NO → Follow-Up (mark Yes/No)
Has the company sent any recent cyber-related communication or guidance?			Were communications integrated into crew training? Yes ☐ / No ☐ Are bulletins stored as FSP documentation? Yes ☐ / No ☐ Were drills conducted based on guidance? Yes ☐ / No ☐	When was the last cyber drill or bulletin issued? Yes ☐ / No ☐ Is the vessel subscribed to company IT/security updates? Yes ☐ / No ☐ Who is the cyber contact at the company? Yes ☐ / No ☐