Facility Name: _____

Facilty Type: _____

Date Coducted: _____

I. Owner or Operator 101.620		SAT	N/O	N/A	FAIL
620(b) 1	Developed Cybersecurity Plan that is approved, and maintained				
620(b) 2	Defined list of personnel attached to cyber responsibilties				
620(b) 3	Records of CySo availble to conact 24 /7 by the Coast Guard				
620(b) 4	Cybersecurity exercises, audits, and inspections, as well as the Cybersecurity Assessment, are conducted as required by this part and in accordance with the Cybersecurity Plan				
620(b) 5	The vessel, facility, or OCS facility operates in compliance with the approved Cybersecurity Plan				
620(b) 6	Cyber Incident Response Plan has been developed approved and exectued				
620(b) 7	All cyber incidents have been properly reported to the National Response Center				

II. Cybersecurity Officer 101.625		SAT	N/O	N/A	FAIL
625(b)	Of all of the the Facilities, Vessels and OSC Facilities, are they all listed within the Cybersecurity Plan of the current facility?				
625(c)	Are any of the responsibilties desginated to other personnel				
625 (d) 1	A Cybersecurity Assessment has been conducted as required				
620(b) 3	The cybersecurity plan has been implemented and conducted and, if needed, conducted.				
625(b) 4	The Cyber Incident Response Plan is executed amd excercised.				
625(b) 5	The Cybersecurity Plan is exercised in accordance with 101.635 (C)				

III. IT Assets 101.650		SAT	N/O	N/A	FAIL
h	Is IT and OT Equipment not segmented networks from each other?				
	Not Sure, please provide details.				
650.b (1)	Do you have an up to date list of all OT and IT assets for the Facility?				
650.b (1)	Do you have a list of IT and OT Asset Inventory Manufacturers?				
650.b (1)	Do you have CCTV (Closed Circuit Television) installed as part of your security system?				
650.b (1)	If yes, is it accessible through a wireless system?				
650.b (1)	Is the CCTV Segmented from other networks of devices?				
650.b (2)	Is there any applications running executable code are disabled by default on critical IT and OT systems;				
650.b (1)	Can you give a list of all software used on IT equipment upon request				
650.b (1)	Can you give a list of all firmware used on IT equipment upon request				
650.b (1)	Can you give a list of all firmware used on OT equipment upon request				
650.b (1)	Can you give a list of all software used on OT equipment upon request				
650.b (3)	Do you have a documented network map and OT device configuration info.				
650.h (1)	Is OT and IT equipment on separate networks from each other?				
650.h (2)	Are all connections between IT and OT systems are logged and monitored for suspicious activity, breaches of security, TSIs, unauthorized access, and cyber incidents.				
650.h (2)	Do you have list all existing 3rd Party Computer Vendors that the facility uses:				
	What are your Internet service providers				

IV. Account Security Measures 101.650.a		SAT	N/O	N/A	FAIL
650.a (1)	Are automatic account lockouts activated after repeated failed log in attempts on all password protected information technology (IT) systems?				
650.a (2)	Are default passwords (or implementing other compensating security controls if unfeasible) changed before using any IT or operational technology (OT) systems?				
650.a (3)	Are there minimum password lengths enforced on all IT and OT systems technically capable of password protection?				
650.a (4)	Is there multifactor authentication being implemented on password-protected IT and remotely accessible OT systems;				
650.a (5)	Is the principle of least privilege to administrator or otherwise privileged accounts on both IT and OT systems?				
650.a (6)	Are there separate user credentials for both critical IT and OT systems;				
650.a (7)	Are user credentials being removed after they leave immediately?				

VI. Cyber Training Records 101.650.c		SAT	N/O	N/A	FAIL
650.c (1)	Are logs securely captured, stored, protected, and accessible only to privileged users?				
	Describe actions taken to create records				
650.c (2)	Is effective encryption deployed to maintain the confidentiality and integrity of IT and OT traffic where technically feasible?				

VIII. Cybersecurity Incident Response Plan 101.650.g		SAT	N/O	N/A	FAIL
650.g (4)	Are Backups being preforms of critical IT and OT systems				
650.g	The Cybersecurity Incident Response Plan lists and identify key roles, responsibilities, and decision-makers				

IX. Cybersecurity Training for Personnel 101.650.d		SAT	N/O	N/A	FAIL
650.d (1)	Does cyber training, for all personnel including contracted workers, include: Recognition/detection of cyber threats and incidents? Cybersecurity measures and techniques? Procedures for reporting ...				
650.d (2)	Do key personnel with access to IT or remote access to OT Equipment have also the following cyber training: Understanding their roles in the event of a cyber incident Up to date knowledge on current events				

X. Cybersecurity Drills 101.635		SAT	N/O	N/A	FAIL
635.b (1)	Are Cybersecurity Drills conducted at least four times every 12 months?				
635.b (1)	Do you keep records of cyber drills preformed?				
635.b (1)	Date of last cybersecurity drill.				
635.c (4)	Did the drill test communication and notification procedures along with any similar elements				
635.c (5)	Was the CySO(s) fully involved in the drill?				
635.c (1)	Is a Cybersecurity Exercise conducted at least annually (no more than 18 months between exercises)?				
635.c (1)	Has a Cyber Assessment been conducted within 24 months of July 16, 2025 (deadline: July 16, 2027)?				
650.e (1) i	Did the assessment reveal any possible vulnerabilities, if so describe them.				

X. Cybersecurity Drills 101.635		SAT	N/O	N/A	FAIL
650.e (1) ii	Have you Validated your most recent Cybersecurity Plan				
650.e (1) iii-v	If there were any recommendations or resolutions conducted, please discuss the execution process.				
650.e (2)	Is Penetration Testing completed when renewing the Cybersecurity Plan?				
660	Does the CySO submit a letter verifying penetration testing completion and identified vulnerabilities?				

XI. Routine Security Maintence 101.650.e		SAT	N/O	N/A	FAIL
650.e (3) i	Is there patching or implementation of documented compensating controls for all KEVs in critical IT or OT systems, without delay, at the time of their annual assessment, as well as part of routine...				
650.e (3) ii	Is there a method to receive and act on publicly submitted vulnerabilities				
650.e (3) iii	Is there a method to share threat and vulnerability information with external stakeholders?				
650.e (3) iii	Is there a method to share threat and vulnerability information with external stakeholders?2				
650.e (3) iv	Are there any exploitable channels directly exposed to internet-accessible systems?				
650.e (3) v	Is there any OT is connected to the publicly accessible internet unless explicitly required for operation, and verify that, for any remotely accessible OT system, there is a documented justificati...				
650.e (3) vi	Have you conducted vulnerability scan per your Cybersecurity Plan.				
650.e (3) ii	Are there limits physical access to OT and related IT equipment to only authorized personnel, and confirm that all HMIs and other hardware are secured, monitored, and logged for personnel access; and				

XII. Routine Security Maintence 101.650.i		SAT	N/O	N/A	FAIL
650.i (1)	Have all unauthorized media and hardware been disconnected from the IT and OT infrastructure, and have all unused physical access ports been blocked, disabled, or removed?				
650.i (2)	Have all unauthorized media and hardware been disconnected from the IT and OT infrastructure, and have all unused physical access ports been blocked, disabled, or removed?				
650.i (2)	If there is any unauthorized media or hardware, what are the procedures for granting access on a by exception basis.				