Port Cyber Alliance · free tool

US Coast Guard cyber rule: what a US terminal must have

Owners and operators of facilities that must have a Facility Security Plan under 33 CFR part 105 (facilities regulated under the Maritime Transportation Security Act, MTSA). The rule also covers U.S.-flagged vessels and Outer Continental Shelf facilities; this checklist is written for facilities only. It does not apply to foreign-flagged vessels (§ 101.605).

Go through the thirteen obligations, fill in the owner, the status and where the evidence is kept, and check the deadline column against the timeline. Section numbers refer to 33 CFR part 101 subpart F. The rule text is the authority: when this checklist and the rule differ, the rule wins.

Guidance, not legal advice. This checklist is guidance written by Port Cyber Alliance from the published rule. It is not legal advice and it does not replace the rule, your Captain of the Port (COTP) or your legal counsel. Port Cyber Alliance does not certify or audit terminals.

On 11 November 2026 we checked eCFR (title 33 up to date as of 9 November 2026): subpart F had not been amended since it took effect on 16 July 2025. The Coast Guard asked in January 2025 for comments on a possible 2-to-5-year delay for U.S.-flagged vessels only; facilities were not part of that question. Check eCFR again before you rely on a date.

Timeline

When	Milestone	Detail
2024-02-22	Proposed rule published (89 FR 13404)	The notice of proposed rulemaking, docket USCG-2022-0802.
2025-01-17	Final rule published (90 FR 6298)	« Cybersecurity in the Marine Transportation System », new subpart F of 33 CFR part 101.
2025-03-18	End of comments on a possible delay for vessels	The question covered U.S.-flagged vessels only, not facilities.
2025-07-16	Rule in force · incident reporting applies	Reportable cyber incidents go to the NRC without delay from this date.
2026-01-12	Training deadline	All personnel and key personnel trained, then every year; new staff within 5 days of access.
2027-07-16	Assessment done, plan submitted, CySO designated	Cybersecurity Assessment completed and Cybersecurity Plan submitted to the COTP; the plan names the CySO.
Plan approval + 60 days	Training on the plan	All personnel trained on the relevant provisions of the approved plan.
Plan approval + 1 year	First annual audit	Then every year, by independent auditors; amendments within 30 days.
Every calendar year	Two drills, one exercise, one assessment	No more than 18 months between exercises; the assessment is also redone on a change of owner.
Plan approval + 5 years	Plan renewal and penetration test	An approved plan is valid 5 years; a penetration test goes with the renewal.

Checklist summary

Obligation	Section	Deadline	Owner	Status
1. Report cyber incidents	§ 101.620(b)(7) · § 101.650(g)(1)	In force since 16 July 2025 (the effective date)		
2. Train all personnel, and key personnel	§ 101.650(d)	By 12 January 2026, then every year. New personnel: within 5 days of getting system access and no later than 30 days after hiring. New IT or OT systems: within 5 days of access. Training on the Cybersecurity Plan itself: within 60 days of the plan's approval.		
3. Designate a Cybersecurity Officer (CySO)	§ 101.620(b)(2)-(3) · § 101.625	By 16 July 2027, within 24 months of the effective date (preamble, section VII). If the CySO changes: tell the Coast Guard and submit the amended part of the plan within 96 hours.		
4. Run the Cybersecurity Assessment	§ 101.650(e)(1)	No later than 16 July 2027, then every year, and sooner if the facility changes owner		
5. Write and submit the Cybersecurity Plan	§ 101.630 · § 101.655	Submitted no later than 16 July 2027. An approved plan is valid 5 years. Amendments go to the Coast Guard at least 30 days before they take effect; a change of owner is written into the plan within 96 hours.		
6. Account and device security	§ 101.650(a)-(b)	Documented in plan sections 6 and 7, submitted by 16 July 2027; then operated as the approved plan says (§ 101.620(b)(5))		
7. Logs and encryption	§ 101.650(c)	Documented in plan section 4, submitted by 16 July 2027		
8. Network segmentation and physical security	§ 101.650(h)-(i)	Documented in plan sections 7 and 8, submitted by 16 July 2027		
9. Vulnerabilities, scans and penetration tests	§ 101.650(e)(2)-(3) · § 101.625(d)(15)	Known exploited vulnerabilities (KEVs): without delay. Scans: as set in the plan (section 6). Penetration test: with each plan renewal (a plan is valid 5 years)		
10. Suppliers and remote connections	§ 101.650(f)	Documented in plan section 4, submitted by 16 July 2027		
11. Incident response plan and backups	§ 101.650(g)(2)-(4) · § 101.620(b)(6)	Documented in plan sections 3 and 9, submitted by 16 July 2027; validation every year		
12. Drills and exercises	§ 101.635	Two drills and one exercise every calendar year under the plan (section 3); no more than 18 months between exercises		
13. Audits, records and communications	§ 101.630(f) · § 101.640 · § 101.645 · § 101.660	First audit no later than 1 year after the plan is approved, then every year		

1. Report cyber incidents

33 CFR § 101.620(b)(7) · § 101.650(g)(1)

Report every reportable cyber incident to the National Response Center (NRC) without delay, unless the incident has already been reported to the Coast Guard under 33 CFR 6.16-1. A reportable cyber incident is one that leads, or could reasonably lead, to a substantial loss of confidentiality, integrity or availability of a covered system, a disruption of operations, a disclosure of personal information of many people, a disruption of critical infrastructure, or a transportation security incident (§ 101.615).

Evidence to hold	Where it is
[ ] A written reporting procedure that names who calls the NRC and when	
[ ] The criteria the team uses to decide that an incident is reportable	
[ ] A log of incidents and of the reports made, with dates and times	

Deadline: In force since 16 July 2025 (the effective date)

2. Train all personnel, and key personnel

33 CFR § 101.650(d)

Everyone with access to IT or OT systems, contractors included, is trained on recognising cyber threats and incidents, the techniques used to get around security measures, how to report an incident to the Cybersecurity Officer, and OT security for those who use OT. Key personnel are also trained on their role during an incident and on keeping up with threats. Anyone not yet trained who must use the systems is accompanied or monitored by a trained person.

Evidence to hold	Where it is
[ ] The training content, by audience (all personnel, key personnel, OT users)	
[ ] Attendance records with names and dates, kept as 33 CFR 105.225 requires	
[ ] The list of key personnel and of contractors with system access	

Deadline: By 12 January 2026, then every year. New personnel: within 5 days of getting system access and no later than 30 days after hiring. New IT or OT systems: within 5 days of access. Training on the Cybersecurity Plan itself: within 60 days of the plan's approval.

3. Designate a Cybersecurity Officer (CySO)

33 CFR § 101.620(b)(2)-(3) · § 101.625

Designate in writing, by name and title, a Cybersecurity Officer who can be reached by the Coast Guard 24 hours a day, 7 days a week, and say how. The CySO may hold other roles and may cover several facilities (each one is listed in each plan). The CySO must have general knowledge of the facility, cybersecurity practice, the plans, audits, training methods, Sensitive Security Information, current threats and known exploited vulnerabilities, and drills (§ 101.625(e)).

Evidence to hold	Where it is
[ ] The written designation, by name and title	
[ ] The 24/7 contact route	
[ ] What shows the CySO's knowledge (training, education or job experience)	
[ ] Section 1 of the plan: the cyber organisation and who does what	

Deadline: By 16 July 2027, within 24 months of the effective date (preamble, section VII). If the CySO changes: tell the Coast Guard and submit the amended part of the plan within 96 hours.

4. Run the Cybersecurity Assessment

33 CFR § 101.650(e)(1)

Analyse all networks to find the vulnerabilities of critical IT and OT systems and the risk of each digital asset, validate the Cybersecurity Plan, record the recommendations in the Facility Security Assessment, patch or put documented compensating controls on every known exploited vulnerability (KEV) in critical systems without delay, and bring the recommendations into the plan by amendment.

Evidence to hold	Where it is
[ ] The assessment report, with the network analysis and the risk per digital asset	
[ ] The list of critical IT and OT systems	
[ ] The KEV list with the patch or compensating control for each	
[ ] The Facility Security Assessment updated with the recommendations	

Deadline: No later than 16 July 2027, then every year, and sooner if the facility changes owner

5. Write and submit the Cybersecurity Plan

33 CFR § 101.630 · § 101.655

The CySO develops the plan; it must describe in detail how every requirement of subpart F is met and contain fourteen sections (organisation and CySO, training, drills and exercises, records, communications, systems and maintenance, access control, physical security, monitoring, audits and amendments, audit reports, unresolved vulnerabilities, incident reporting, the Cybersecurity Assessment). It can sit in the Facility Security Plan, in an annex or in a separate submission, and it is Sensitive Security Information (49 CFR part 1520). One copy goes to the cognizant COTP or OCMI for approval.

Evidence to hold	Where it is
[ ] The plan, with an index if the sections are not in the rule's order	
[ ] The proof of submission to the COTP and the Coast Guard's reply letter	
[ ] SSI handling for the plan (who may read it, where it is kept)	

Deadline: Submitted no later than 16 July 2027. An approved plan is valid 5 years. Amendments go to the Coast Guard at least 30 days before they take effect; a change of owner is written into the plan within 96 hours.

6. Account and device security

33 CFR § 101.650(a)-(b)

Account lockout after repeated failed logins on IT systems; default passwords changed before use (or documented compensating controls); a minimum password strength; multifactor authentication on password-protected IT and on remotely accessible OT (or documented compensating controls); least privilege for privileged accounts; separate credentials on critical systems; credentials removed when a user leaves. A list of approved hardware, firmware and software; executable code disabled by default on critical systems; an inventory of network-connected systems; a network map and OT device configuration documentation.

Evidence to hold	Where it is
[ ] The account policy and screenshots or exports showing lockout, MFA and password settings	
[ ] The compensating controls where a measure is not feasible	
[ ] The approved hardware and software list, the asset inventory, the network map	
[ ] Leaver records showing credentials revoked	

Deadline: Documented in plan sections 6 and 7, submitted by 16 July 2027; then operated as the approved plan says (§ 101.620(b)(5))

7. Logs and encryption

33 CFR § 101.650(c)

Logs are securely captured, stored and protected so that only privileged users can reach them. Effective encryption protects sensitive data and the integrity of IT and OT traffic when technically feasible.

Evidence to hold	Where it is
[ ] Where the logs go, who can read them, how long they are kept	
[ ] The encryption in place for sensitive data and traffic, and the cases judged not feasible	

Deadline: Documented in plan section 4, submitted by 16 July 2027

8. Network segmentation and physical security

33 CFR § 101.650(h)-(i)

Segment IT and OT networks, and log and monitor every connection between them. Limit physical access to OT and related IT equipment to authorised people, secure and log access to HMIs and other hardware, keep unauthorised media and hardware off the systems and block or remove unused ports.

Evidence to hold	Where it is
[ ] The network diagram showing the IT/OT boundary	
[ ] The logs or monitoring of IT-OT connections	
[ ] The physical access list for OT rooms and the port-blocking procedure	

Deadline: Documented in plan sections 7 and 8, submitted by 16 July 2027

9. Vulnerabilities, scans and penetration tests

33 CFR § 101.650(e)(2)-(3) · § 101.625(d)(15)

Patch or put documented compensating controls on every KEV in critical systems without delay. Keep a way to receive and act on vulnerabilities reported by the public, and a way to share threat information with external stakeholders. No exploitable channel exposed to the internet; no OT on the public internet unless required, with a documented justification for any remotely accessible OT. Run vulnerability scans as the plan says. A penetration test is done in conjunction with each plan renewal, and a letter certifying it, with every vulnerability found, goes into the Facility Security Assessment.

Evidence to hold	Where it is
[ ] KEV tracking with dates of patch or compensating control	
[ ] The public vulnerability reporting contact	
[ ] The justification for each remotely accessible OT system	
[ ] Scan reports; the penetration test letter at renewal	

Deadline: Known exploited vulnerabilities (KEVs): without delay. Scans: as set in the plan (section 6). Penetration test: with each plan renewal (a plan is valid 5 years)

10. Suppliers and remote connections

33 CFR § 101.650(f)

Use cybersecurity capability as a criterion when buying IT and OT systems or services. Set up a process so that every IT and OT vendor or service provider tells you of vulnerabilities and reportable cyber incidents without delay. Monitor and document all third-party remote connections.

Evidence to hold	Where it is
[ ] The cyber criteria in your procurement documents	
[ ] The vendor notification clause or process	
[ ] The register of third-party remote connections and their monitoring	

Deadline: Documented in plan section 4, submitted by 16 July 2027

11. Incident response plan and backups

33 CFR § 101.650(g)(2)-(4) · § 101.620(b)(6)

Develop, implement, maintain and exercise a Cyber Incident Response Plan. Validate the Cybersecurity Plan every year through exercises, reviews of incident response cases or a post-incident review. Back up critical IT and OT systems; protect the backups and test them often.

Evidence to hold	Where it is
[ ] The Cyber Incident Response Plan, with roles and decision-makers	
[ ] The yearly validation record	
[ ] Backup scope, protection and restore test records	

Deadline: Documented in plan sections 3 and 9, submitted by 16 July 2027; validation every year

12. Drills and exercises

33 CFR § 101.635

At least two cybersecurity drills each calendar year, each testing elements of the plan. At least one exercise each calendar year, with no more than 18 months between exercises; it can be live, tabletop or combined with other security exercises, and the CySO takes an active part. A real incident handled under the plan can count if the goals are reached and documented.

Evidence to hold	Where it is
[ ] Drill and exercise reports with dates, scenario, participants	
[ ] Corrective actions and when they were closed	

Deadline: Two drills and one exercise every calendar year under the plan (section 3); no more than 18 months between exercises

13. Audits, records and communications

33 CFR § 101.630(f) · § 101.640 · § 101.645 · § 101.660

An audit of the plan and its implementation every year, by people who are independent of the measures audited, plus an audit when the owner or the measures change; amendments from an audit go to the Coast Guard within 30 days. Records are kept for training, drills, exercises, threats, reportable incidents and audits (33 CFR 105.225). The CySO can tell owners and staff of changes in cyber conditions. The plan and penetration test results are available to the Coast Guard on request.

Evidence to hold	Where it is
[ ] The yearly audit report attached to the plan	
[ ] The records register	
[ ] The communication means written in plan section 5	

Deadline: First audit no later than 1 year after the plan is approved, then every year

Sources (public, dated)

Federal Register, 90 FR 6298, Cybersecurity in the Marine Transportation System, final rule (doc. 2025-00708, docket USCG-2022-0802), 17 January 2025. https://www.federalregister.gov/documents/2025/01/17/2025-00708/cybersecurity-in-the-marine-transportation-system

Official text (PDF), Federal Register Vol. 90 No. 11, pages 6298-6453; subpart F at pages 6447-6453, 17 January 2025. https://www.govinfo.gov/content/pkg/FR-2025-01-17/pdf/2025-00708.pdf

eCFR, 33 CFR part 101 subpart F, Cybersecurity (§§ 101.600-101.670), in force since 16 July 2025, checked 11 November 2026. https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F

Regulations.gov, docket USCG-2022-0802, rulemaking docket, 2024-2025. https://www.regulations.gov/docket/USCG-2022-0802

Federal Register, 89 FR 13404, notice of proposed rulemaking, 22 February 2024. https://www.federalregister.gov/documents/2024/02/22/2024-03075/cybersecurity-in-the-marine-transportation-system

Licence

Creative Commons Attribution 4.0 International (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/ . You may copy, adapt and share this checklist, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/resources/compliance-center/uscg-cyber-rule-checklist/ . Generic: no terminal, port, client or vendor is named, no figure is invented. This checklist is guidance, not legal advice; the rule text is the authority. Port Cyber Alliance does not certify or audit terminals.