FREE ASC RESOURCE · UPDATED NOVEMBER 22, 2026

Cybersecurity Plan Readiness Checklist

USCG 33 CFR Part 101, Subpart F · updated for NVIC 02-26

For Facility Security Officers, Cybersecurity Officers and port, terminal and vessel operators preparing for the Coast Guard's maritime cyber rule. Every item ties to its section of the rule, so you can see exactly what is required and where to find it.

Prefer to automate it?

Instead of gathering the evidence by hand, use ccSentinel, ASC's Subpart F platform. It imports your scan data, flags Known Exploited Vulnerabilities, maps findings to the rule and produces reports to build your Cybersecurity Plan from.

Learn more at cc-sentinel.com

Key dates

July 16, 2025

Rule in effect

Reportable cyber incidents go to the National Response Center without delay.

§ 101.650(g)(1)

January 12, 2026

Training required

All personnel with IT or OT access, and key personnel, trained; then annually. Still in effect before your Plan is filed. If yours is not done, close the gap now and document it.

§ 101.650(d)(4)

July 16, 2027

Assessment and Plan due

Cybersecurity Assessment complete and Cybersecurity Plan submitted. From this date you operate under your submitted Plan.

§ 101.655

After approval

Ongoing cycle

Plan-provisions training within 60 days; annual audit, Assessment, drills and exercise; penetration test before each 5-year renewal.

§ 101.630(f)(1)

How to use this checklist

Work through each area with your FSO, IT and OT leads. Check an item when it is in place *and* documented, since the Coast Guard will look for both. Each citation links to the rule text on eCFR. Section tags follow the Coast Guard's preferred Plan layout (NVIC 02-26, Enclosure 1, Table 1). Gold-labeled notes summarize what NVIC 02-26 adds.

Build your Plan faster with ccSentinel

Much of this checklist comes down to evidence: asset inventories, vulnerability findings, KEV status and a written account of how you meet each requirement. ccSentinel, ASC's Subpart F platform, automates that work so your team can build the Cybersecurity Plan in less time.

1 Import
Drag in SIW XML or Nessus, Rapid7, Action1, Yokogawa, Phosphorus or Companion data. Assets are assigned to each facility or vessel.

2 Detect and map
Findings are checked against the CISA KEV catalog (refreshed every 6 hours) and mapped to the Subpart F control areas.

3 Report
Generate print-ready reports with KEV matches, per-system detail, network topology maps and a compliance narrative to build your Plan from.

Free for organizations with up to 3 facilities and fewer than 200 endpoints. No credit card required.

1 Cybersecurity Officer and organization

Plan Section 1 Name who owns cybersecurity, early, and make sure the Coast Guard can reach them.

- [ ] Designate a Cybersecurity Officer (CySO) in writing, by name and by title.

  § 101.620(b)(3)

  NVIC 02-26 Designate the CySO early so they can guide the Assessment and critical-system decisions. Enclosure (2) has an optional sample designation letter.

- [ ] Confirm the CySO is reachable by the Coast Guard 24 hours a day, 7 days a week, and document how to contact them at any time.

  § 101.620(b)(3)

- [ ] Designate one or more alternate CySOs and give the Coast Guard their contact information the same way.

  § 101.615

  NVIC 02-26 Each alternate must meet the same qualifications as the primary CySO.

- [ ] Verify the CySO has general knowledge, through training, education or experience, in each of the 12 areas the rule lists.

  § 101.625(e)

  NVIC 02-26 No specific certification or U.S. citizenship is required. Designating a CySO affirms to the Coast Guard that they qualify. The role can be filled in-house or by a contractor.

- [ ] If one person is CySO for several facilities or vessels, list every one of them in each Plan, and confirm the workload is manageable.

  § 101.625(b)

- [ ] Define the cybersecurity organizational structure and identify each person with cybersecurity duties.

  § 101.620(b)(2)

  ASC TIP Include the FSO or VSO and your IT and OT engineers; the NVIC expects them to work with the CySO.

- [ ] Set up a process to notify the Coast Guard within 96 hours of a CySO (or alternate) change and submit the amended Plan section.

  § 101.630(e)(4)

- [ ] Set up a process to amend the Plan within 96 hours of a change in owner or operator.

  § 101.630(e)(3)

2 Cybersecurity Assessment

Plan Sections 11, 12 and 14 The Assessment sets the scope of the Plan. Do it first. It is due by July 16, 2027, then annually.

- [ ] Schedule the Cybersecurity Assessment to finish well before July 16, 2027, leaving time to write the Plan from its results.

  § 101.650(e)(1)

  NVIC 02-26 The Coast Guard recommends completing the Assessment before drafting the Plan.

- [ ] Inventory all systems, dependencies and interfaces, including cloud services, vendor connections, landlord networks and BYOD, not just the obviously critical systems.

  § 101.650(e)(1)(i)

  NVIC 02-26 Enclosure (4) sorts assets into internal networks, external dependencies and interfaces.

- [ ] Analyze all networks to identify vulnerabilities to critical IT and OT systems and the risk posed by each digital asset, using both technical and qualitative methods.

  § 101.650(e)(1)(i)

  NVIC 02-26 A visual check or cursory review is not enough. Name the standard you used (for example, the NIST CSF) in the Assessment report.

- [ ] Designate critical IT and OT systems: any system whose compromise could result in a transportation security incident. Treat “maybe” answers as critical.

  § 101.615

  NVIC 02-26 The NVIC’s “maybe” examples include tank level sensors, badge access servers and cargo release systems.

- [ ] Use the Assessment to validate the Cybersecurity Plan.

  § 101.650(e)(1)(ii)

- [ ] Document recommendations and resolutions in the FSA or VSA, and fold them into the Plan through an amendment.

  § 101.650(e)(1)(iii)

- [ ] Document patching or compensating controls for every Known Exploited Vulnerability (KEV) found in critical IT or OT systems.
  § 101.650(e)(1)(iv)

- [ ] If one Plan covers several facilities or vessels, complete an individual Assessment for each.
  § 101.630(d)(2)

- [ ] Mark and handle the Assessment report as SSI, and include the current version in Plan Section 14.
  § 101.630(c)(14)

- [ ] Repeat the Assessment annually, and sooner if ownership changes.
  § 101.650(e)(1)

- [ ] If you will seek a waiver or equivalency, complete the Assessment first.
  § 101.665
  NVIC 02-26 A rigorous, standards-based Assessment is strongly recommended to support the request.

3 Writing and submitting the Plan

All sections Structure, protection and submission of the Cybersecurity Plan itself.

- [ ] Include all 14 required sections in the rule's order, or add an index showing where each one is.
  § 101.630(c)
  NVIC 02-26 The Coast Guard prefers the Table 1 crosswalk. If you use it, say so on the first page. Keep the Cyber Incident Response Plan as an appendix.

- [ ] Describe specifically how each Subpart F requirement is met, tied to the risks found in the Assessment. Do not just restate the rule.
  § 101.630(a)

- [ ] Choose the format: within the FSP or VSP, as an annex, as a separate submission, or through an approved Alternative Security Program.
  § 101.630(a)
  NVIC 02-26 The Coast Guard recommends submitting the Plan as a discrete, cohesive package.

- [ ] Where a requirement cannot be met as written and the rule does not allow compensating controls, prepare a waiver or equivalency request.
  § 101.665

- [ ] Mark and protect the Plan as Sensitive Security Information (SSI) under 49 CFR Part 1520, and keep it out of public AI tools.
  § 101.630(b)

- [ ] For landlord and tenant arrangements, do a joint review of who owns which IT and OT systems, and decide on separate Plans or a combined-Plan equivalency.

  § 101.630(a)

- [ ] If one Plan covers several similar facilities or vessels, address each one's specific risks and include everything needed to serve as a full Plan for each.

  § 101.630(d)(2)

- [ ] Submit the Plan by July 16, 2027: to the Captain of the Port or OCMI for facilities and OCS facilities, or as directed for vessels.

  § 101.655

  NVIC 02-26 Submissions use DoD SAFE under Coast Guard work instruction MCP-WI-003. For vessels, the NVIC routes Plans to the Office of Maritime Cybersecurity Policy (CG-MCP). The rule text still names the Marine Safety Center.

- [ ] After submitting, review cybersecurity content in your existing FSP or VSP and amend it if the new Plan supersedes it.

  § 101.630(e)

- [ ] Track the 5-year approval period so renewal and its penetration test are planned in advance.

  § 101.630(d)(3)

- [ ] Send proposed amendments at least 30 days before they take effect. For exigent changes, notify the Coast Guard by the fastest practicable means.

  § 101.630(e)(2)

- [ ] Keep the Plan and penetration test results ready to show the Coast Guard on request.

  § 101.660

4 Training and awareness

Plan Section 2 Training has been required since January 12, 2026. Confirm everyone is covered and that you can prove it.

- [ ] Identify everyone with access to IT or OT systems, including contractors and anyone with physical access to spaces housing IT or OT equipment.

  § 101.650(d)(1)

  NVIC 02-26 Physical access alone counts as access.

- [ ] Train all of them on recognizing threats and incidents, techniques used to circumvent security, and how to report an incident to the CySO. Then repeat annually.

  § 101.650(d)(4)

  NVIC 02-26 Until July 16, 2027, follow CG-5PC Policy Letter 01-25.

- [ ] Provide OT-specific cybersecurity training for everyone whose duties include using OT.

  § 101.650(d)(1)(v)

- [ ] Name your key personnel by position or name, with your reasoning, and train them on incident roles and on keeping current with threats.

  § 101.650(d)(2)

  NVIC 02-26 Examples: leadership, CSO, FSO, VSO, admins, OT engineers with elevated access, and the CySO.

- [ ] Train all personnel on the relevant provisions of the Plan within 60 days of Plan approval.

  § 101.650(d)(4)

- [ ] Train new personnel within 5 days of gaining system access and no later than 30 days after hiring; train on new IT or OT systems within 5 days of access.

  § 101.650(d)(4)

- [ ] Escort or monitor anyone who needs access before completing training. Describe any remote “escorting” method (for example, session shadowing or recording) in the Plan.

  § 101.650(d)(3)

- [ ] For contractors, train them, escort them, or evaluate and document their company’s training program and re-review it annually.

  § 101.650(d)(1)

- [ ] Keep training records showing the date, duration, an outline mapped to each required topic, and attendees.

  § 101.640

  NVIC 02-26 If learning-system module titles don’t match the rule’s topics, keep a cross-reference.

5 Drills and exercises

Plan Section 3 Test the Plan and the people who run it.

- [ ] Conduct cybersecurity drills at least twice each calendar year, testing a different Plan element each time, including responses to threats and incidents.

  § 101.635(b)(1)

  NVIC 02-26 Space drills evenly through the year. They may be combined with existing MTSA drills.

- [ ] Conduct an exercise at least once each calendar year, with no more than 18 months between exercises: full-scale, live, tabletop or combined.

  § 101.635(c)(1)

- [ ] Test communication and notification procedures, coordination, resource availability and response in each exercise, with the CySO actively participating.
  § 101.635(c)(4)

- [ ] If you combine cyber and physical security exercises, or exercise the Incident Response Plan with the Plan, make sure the record documents both.
  § 101.635(c)(2)

- [ ] For joint port or tenant exercises, confirm the scenario fully tests your own Plan and document it.
  § 101.635(c)(3)

- [ ] Address and document corrective actions from exercises as soon as possible.
  § 101.635(c)(6)

- [ ] If a real incident response is used to satisfy a drill or exercise, document how its goals were met and make the record available to the COTP.
  § 101.635(a)(2)

6 Records and communications

Plan Sections 4 and 5 Keep the evidence, and make sure word gets out when conditions change.

- [ ] Keep records of training, drills, exercises, cybersecurity threats observed, reportable cyber incidents and audits.
  § 101.640
  NVIC 02-26 Also treat the approved list, inventory, network map and penetration test letter as records if kept outside the Plan.

- [ ] Document how electronic and paper records are protected as SSI, with need-to-know access controls.
  § 101.630(b)

- [ ] Document how the CySO notifies owners, operators and personnel of changes in cybersecurity conditions, including a fallback if email or VoIP is down.
  § 101.645(a)

- [ ] Maintain continuous communications with security personnel, interfacing vessels, the COTP and authorities with security responsibilities.
  § 101.645(b)

7 Systems, equipment and maintenance

Plan Section 6 Know what is on your network, control what gets installed, and keep it patched and backed up.

- [ ] Maintain a signed or electronically approved list of hardware, firmware and software, including OT and ICS (PLCs, HMIs, SCADA, telemetry), and allow only listed items.

  § 101.650(b)(1)

  NVIC 02-26 Include enough detail to verify a model or version: name, version, manufacturer, approval and review dates, criticality.

- [ ] Disable applications that run executable code by default on critical IT and OT systems.

  § 101.650(b)(2)

- [ ] Maintain an accurate inventory of network-connected systems, with critical IT and OT systems designated, including any BYOD devices or your MDM policy.

  § 101.650(b)(3)

- [ ] Maintain an accurate network map, showing IT–OT segmentation, and OT device configuration documentation.

  § 101.650(b)(4)

- [ ] Patch or apply documented compensating controls for KEVs in critical IT and OT systems without delay.

  § 101.650(e)(3)(i)

  NVIC 02-26 "Without delay" means urgent action as soon as reasonably and safely possible. Use CISA's KEV Catalog, and address KEVs on all systems too.

- [ ] Define and run vulnerability scans with a stated frequency, method and scope.

  § 101.650(e)(3)(vi)

- [ ] Publish a way for outsiders to report vulnerabilities to you, with internal handling steps and response timelines.

  § 101.650(e)(3)(ii)

- [ ] Maintain a way to share threat and vulnerability information with external stakeholders.

  § 101.650(e)(3)(iii)

  NVIC 02-26 The NVIC points to Area Maritime Security Committees, FBI InfraGard and CISA alerts. Sharing does not replace required reporting.

- [ ] Find and close exploitable channels exposed to internet-accessible systems: network, removable media, wireless and vendor pathways.

  § 101.650(e)(3)(iv)

  NVIC 02-26 Combine discovery scans, vulnerability scans and physical walk-downs.

- [ ] Keep OT off the public internet unless operationally required, and document the justification for any remotely accessible OT.
  § 101.650(e)(3)(v)

- [ ] Make cybersecurity capability an evaluation criterion when buying IT and OT systems or services.
  § 101.650(f)(1)

- [ ] Back up critical IT and OT systems, protect the backups and test restores frequently, with recovery time and point objectives where practical.
  § 101.650(g)(4)

8 Access control, physical security and monitoring

Plan Sections 7, 8 and 9 Who can log in, who can touch the equipment, and how you would know.

- [ ] Enable automatic account lockout after repeated failed logins on all password-protected IT systems.
  § 101.650(a)(1)

- [ ] Change default passwords before any IT or OT system is used. Where that is not feasible, document compensating controls.
  § 101.650(a)(2)

- [ ] Enforce a minimum password strength on all IT and OT systems capable of password protection.
  § 101.650(a)(3)

- [ ] Implement multifactor authentication on password-protected IT systems and remotely accessible OT systems. Where not feasible, document compensating controls.
  § 101.650(a)(4)

- [ ] Apply least privilege to administrator and other privileged accounts on IT and OT systems, and keep separate credentials on critical systems.
  § 101.650(a)(5)

- [ ] Remove or revoke credentials when a user leaves the organization.
  § 101.650(a)(7)
  ASC TIP Tie this to HR offboarding and include contractor accounts.

- [ ] Segment IT networks from OT networks (logical controls in Section 7, physical separation such as air gaps in Section 8).
  § 101.650(h)(1)

- [ ] Log and monitor all IT–OT connections for suspicious activity, breaches, unauthorized access, TSIs and cyber incidents.
  § 101.650(h)(2)

- [ ] Capture, store and protect logs so only privileged users can access them.
  § 101.650(c)(1)

- [ ] Use effective encryption for sensitive data and IT and OT traffic where technically feasible.
  § 101.650(c)(2)

- [ ] Limit physical access to OT and related IT equipment, including HMIs, to authorized personnel; secure, monitor and log that access and review the logs.
  § 101.650(i)(1)

- [ ] Block, disable or remove unused ports and keep unapproved media and hardware off IT and OT, with a by-exception approval procedure.
  § 101.650(i)(2)

- [ ] Monitor and document all third-party remote connections to detect cyber incidents.
  § 101.650(f)(3)

9 Audits, amendments and vulnerability tracking

Plan Sections 10, 11 and 12 Prove the Plan works, track every finding and keep the Plan current.

- [ ] Audit the Plan and its implementation annually, starting within 1 year of approval, and attach a certifying report.
  § 101.630(f)(1)

- [ ] Use an auditor who knows audit methods, has no regular cybersecurity duties at the site and is independent of the measures audited. The CySO arranges the audit but does not conduct it.
  § 101.630(f)(4)

- [ ] Audit again after a change in owner or operator or a change to cybersecurity measures.
  § 101.630(f)(2)

- [ ] Submit any audit-driven Plan amendments within 30 days of completing the audit.
  § 101.630(f)(5)

- [ ] Keep a consolidated list of vulnerabilities from the Assessment, scans, penetration tests and KEVs, with how each was resolved or mitigated.
  § 101.630(c)(11)
  NVIC 02-26 A living document, not on form CG-6025. Adding entries does not by itself require a Plan amendment.

- [ ] Document every unresolved vulnerability, including risk acceptance decisions with reasoning or a target completion date.

  § 101.630(c)(12)

- [ ] Plan a penetration test at least once per 5-year cycle, ideally within 24 months before renewal, and include the certifying letter and findings in the FSA or VSA.

  § 101.650(e)(2)

  NVIC 02-26 Not required for the initial July 2027 submission. Where live OT testing is unsafe, test the OT boundary.

- [ ] Arrange cybersecurity inspections and promptly correct problems found in exercises, audits and inspections.

  § 101.625(d)(6)

10 Incident reporting and response

Plan Section 13 and CIRP appendix Know what to report, who reports it and how you recover.

- [ ] Make sure staff know what counts as a reportable cyber incident.

  § 101.615

  NVIC 02-26 NVIC 02-24 (series) harmonizes the incident definitions in 33 CFR Parts 6 and 101.

- [ ] Report reportable cyber incidents to the National Response Center (1-800-424-8802) without delay, unless already reported under 33 CFR 6.16-1.

  § 101.650(g)(1)

- [ ] Name who (by position or name) makes outside notifications, and list NRC and COTP contact information in the Plan.

  § 101.620(b)(7)

  ASC TIP Tenants should coordinate reporting with the landlord port.

- [ ] Require all IT and OT vendors and service providers to notify you of vulnerabilities and reportable cyber incidents without delay.

  § 101.650(f)(2)

  ASC TIP Add this to contracts and renewal terms.

- [ ] Ensure the CySO records all reportable cyber incidents and reports them to the owner or operator, and records actual threats the site has observed.

  § 101.625(d)(10)

- [ ] Develop, implement, maintain and exercise a Cyber Incident Response Plan covering detection through recovery and lessons learned, with roles and decision-makers named.

  § 101.650(g)(2)

  NVIC 02-26 Updating the Incident Response Plan does not require a Plan amendment, but include it in audits.

- [ ] Validate the Plan periodically through annual exercises, reviews of incident cases or post-incident reviews.

  § 101.650(g)(3)

What NVIC 02-26 changes for you

On October 19, 2026 the Coast Guard issued NVIC 02-26, its implementation guidance for Subpart F. It does not create new legal requirements, but it shows how inspectors will read the rule. Points to note:

- NVIC 01-20 (cyber risk in Facility Security Plans) is cancelled. Policy Letter 01-26 (Assessment scoping) is folded into the NVIC. Policy Letter 01-25 (training) stays in effect until July 16, 2027.
- Compensating controls are allowed only where the rule says so (default passwords, MFA, KEVs). Anywhere else, a requirement you cannot meet as written needs a waiver or equivalency request under § 101.665.
- Restating the regulation is not enough. The Plan must say how you specifically meet each requirement, and inspectors will look for documentation and observable evidence.
- For training, “access” includes physical access to spaces housing IT or OT equipment, not just logins.
- The Coast Guard recommends completing the Assessment before drafting the Plan, and every facility or vessel needs its own Assessment, even under a shared Plan.
- No penetration test is required with the initial July 2027 submission. One is required at least once per 5-year cycle, ideally within 24 months before renewal.
- For Plans approved before July 16, 2027, annual timelines (audits, Assessments, drills, exercises) run from July 16, 2027.
- Landlord ports and tenants should jointly review who owns which systems. Each Part 105 facility needs its own Plan or an approved equivalency.
- Do not paste the Plan, Assessment or other SSI into public AI tools. The NVIC treats that as an unauthorized disclosure under 49 CFR Part 1520.

Questions to the Coast Guard: MTSCyberRule@uscg.mil (Office of Maritime Cybersecurity Policy).

About this resource. This checklist is an educational resource from Applied Security Convergence (ASC). It is based on the public text of 33 CFR Part 101, Subpart F (eCFR, current as of October 30, 2026) and Coast Guard NVIC 02-26 (October 19, 2026). It is not legal advice and does not replace the rule, Coast Guard guidance, or direction from your Captain of the Port, OCMI or the Marine Safety Center. Where this checklist and the rule differ, the rule controls.

https://www.appsecconv.com/resources/subpart-f-checklist · © 2026 Applied Security Convergence