COVERAGE AND OWNERSHIP

Identify the operator and the plan

Use one copy per vessel or facility. Enter document references, dates and role titles. Keep actual manifests, plan contents, sensitive diagrams and credentials in their approved systems.

First decision

For a U.S. flagged passenger vessel, check whether Part 104 requires a security plan. For a shoreside terminal check Part 105. For foreign flagged ships, review applicable flag, safety management and port requirements. A port call alone does not establish Subpart F coverage.

Vessel or facility identifier, flag or facility type, and operation in scope

Plan owner and security officer role / 24 hour contact directory reference

Applicable rule, contract or flag basis and record supporting the decision

What is inside the boundary? Which tenant or shoreside provider shares responsibility?

Open coverage question, who will resolve it, and by what date

Primary references

Subpart F Vessel coverage Facility coverage IMO cyber risk

© 2026 Global Digital Forensics, Inc. All rights reserved.

CALENDAR AND EVIDENCE

Plan the assessment and annual audit

Use the date on the Coast Guard correspondence. Name an owner for every date and keep the evidence reference alongside the entry.

Milestones for covered operators

Initial role based training fell due January 12, 2026. By July 16, 2027, designate the CySO, complete the initial assessment and submit the plan. Prepare to operate to the requirements and submitted plan by then. The assessment recurs annually and earlier on ownership change.

Set the audit schedule separately

For early plan approvals NVIC 02-26 uses July 16, 2027 as the recurring schedule anchor. Otherwise apply the approval based timetable in § 101.630(f). Check for changes that require an additional audit. Document auditor qualifications, duties and independence.

Training roster reference, contractor coverage, most recent and next training dates

CySO designation, assessment completion date, next assessment and owner

Plan submission and approval dates, correspondence reference, next audit and basis

Two drills each calendar year and annual exercise (maximum interval 18 months): dates and records

Audit lead, independence check, missing evidence or scheduling decision

Primary references

Rule and audit requirements Coast Guard implementation guidance Signed copy

© 2026 Global Digital Forensics, Inc. All rights reserved.

IT AND OPERATIONAL TECHNOLOGY

Follow one operating function

Choose one navigation, engineering, boarding, baggage, gate or cargo function that matters on a working shift. Select records with the master or terminal lead. Use a new copy of this page for the next sample.

What good evidence looks like

A dated vendor work order names the authorizing officer and system. An access record covers the service window. The operations lead records a check before return to service. A crew approved fallback or current recovery record shows how the operation can continue.

Function, accountable officer, business dependency and effect of loss

Asset or service reference, custodian, vendor and authorized working limits

Access approval and removal: document references, dates and reviewer

Segmentation, backup or fallback: record reviewed, date and result

What the available evidence demonstrates, what is missing and who will supply it

Primary references

33 CFR 101.650 Coast Guard implementation guide IMO cyber risk guidance

© 2026 Global Digital Forensics, Inc. All rights reserved.

INFORMATION AND REPORTING

Trace a record and rehearse the calls

Select a passenger, crew, visitor or workforce record type. Record the field category and custodian only. The privacy lead and duty officer can use this sheet together.

Check both reporting decisions

For actual or threatened cyber incidents under 33 CFR 6.16-1, report immediately: NRC 800-424-8802 and separately CISA 844-729-2472. For a transportation security incident, Part 104 and 105 operators notify the local COTP without delay; Part 106 operators notify the cognizant District Commander without delay. Then follow the security plan immediately. Have the CySO and counsel separately assess the maritime personal information trigger and applicable privacy clocks.

Record category, collector, ship to shore or supplier handoff, retention owner

Access review reference, evidence date, disposition or deletion check

Maritime reporting decision, time, officer, authority and reference

Privacy assessment: affected jurisdiction, trigger or clock, counsel and next decision

Alternate duty contact directory reference, last exercise and open issue

Primary references

USCG incident reporting 33 CFR 6.16-1 Florida § 501.171

© 2026 Global Digital Forensics, Inc. All rights reserved.

FINDING AND VERIFIED CLOSURE

Give every open item a finish line

Use a copy for each finding. Leadership should be able to identify the effect on operations, the person who can fix the gap and the evidence required to close it.

Example of a usable finding

The sampled vendor maintenance record shows authorization but no record of access ending. The terminal operations manager requests the closure record from the provider by the agreed date. The reviewer compares that record to the authorized window and records the result.

Plan section or requirement, sampled evidence reference and date

Condition found, affected function or information and operational consequence

Action, accountable owner and target date

Closure evidence, independent reviewer, verification date and disposition

Plan amendment needed? Record CySO decision, 30 day deadline if applicable and submission reference

Primary references

Plan audits and amendments Coast Guard crosswalk Sensitive Security Information

© 2026 Global Digital Forensics, Inc. All rights reserved.