Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/maritime-assessment-preparation/

A PLANNING GUIDE FOR PORT AUTHORITIES, TERMINAL OPERATORS AND VESSEL OPERATORS

Prepare for a Maritime Cybersecurity Assessment Before Testing Starts

A port assessment runs smoothly when three things are settled early: who authorizes work on a tenant's crane controls, how current the network diagram is, and which safeguards are agreed before any active test is proposed. This guide settles authority, records and safeguards first, and (800) 868-8189 reaches a senior practitioner for everything else.

Name the Decision the Assessment Has to Support

Start with the decision, then the technology. An initial assessment, an update to existing work, a verification of selected corrections and a recovery review each produce a different record, and scoping for the right one gives management a report built around its question. Write down what is due, who will decide it, which planning or submission dates sit behind it and who confirms those dates, and treat that page as the first artifact of the engagement.

Regulatory applicability is settled by the responsible owner and its advisers, and the technical team works from their decision. The question for a port or vessel is whether the owner or operator is required to hold a security plan, because the Coast Guard cybersecurity obligations in 33 CFR part 101, subpart F attach through that plan: personnel training was due by January 12, 2026, and the first Cybersecurity Assessment and the Cybersecurity Plan submission are due no later than July 16, 2027. A technical review becomes part of a regulatory assessment once the person with authority to say so has confirmed what the rule requires of this facility or this vessel, and the file records who that person was.

Four questions sort most of this out before we speak. What decision is due, and who will make it? What work already exists, and which questions remain open? Which findings, changes or operational dependencies need attention now? And what evidence would make the result useful to both management and the technical staff who will act on it? Answers to all four give the report its shape, so it serves the decision as well as the date.

If the four questions produce four different answers inside your organization, bring them to the scope conversation as they stand; sorting them is part of the work.

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

Map the Facility, Its Systems and Who Authorizes Each

In a working port the authority, the terminal operator, the tenants and the equipment vendors each control a different part of the same environment, and a vessel alongside brings its own operator and its own networks. For every relevant system record who owns it, who operates it day to day and who can authorize its examination, because the tenant's crane controls, the vendor's remote gateway and the ship's bridge network each carry their own permission, separate from that of the entity that commissioned the assessment. The artifact is a system list with three owner columns, and a name in every column is what lets the assessment move from system to system.

Include the supporting business services, identity, communications and outside connections wherever they affect operations: the terminal operating system and its vendor support link, the gate and access control systems, the crane and straddle carrier control networks, reefer monitoring, shore power, the radio and cellular links to the yard, and the identity directory that the operational workstations authenticate against. Draw the boundaries between separately owned or managed systems explicitly, each system in its own box. Those boundaries are where the examiner looks first for shared responsibilities and access paths, and a diagram drawn that way gives the work a head start.

For the scoping call, prepare a general description of the facility and its operations, the relevant IT and OT systems with their critical operational dependencies, the owner, operator, tenant and vendor responsibilities for each, and the access authority, excluded systems and third party permission requirements that will shape what can be examined. Expect to be asked for the current network drawing and the date it was last verified against the equipment on the pier; the honest date is what the examiner works from.

Whether the boundaries between those networks actually hold is what network segmentation validation tests, once authority over each one is settled.

Bring the People Who Approve Scope and Hold Stop Authority

Identify the owner or engagement sponsor, the Cybersecurity Officer where one applies, the security lead, the operations and engineering contacts, the IT administrator and the relevant vendor contacts. Then decide, before the work is agreed, who approves methods, who can stop the work and who receives an urgent finding at two in the morning. Write the names and the alternates on one page with a tested phone number for each, so a stop authority is reachable throughout the site week.

Specialist legal, regulatory and engineering responsibilities each have a named owner, and they stay with that owner throughout the assessment. A scope that says so plainly gives everyone a clear position when a decision is explained to the Coast Guard, an insurer or a court. The examiner will ask who signs the applicability decision, who approves any active method on a crane or a vessel system and who accepts the residual risk the report identifies, and the answer to each question is a named person.

Name those people first; then call (800) 868-8189 and a senior practitioner will agree on the approval and stop arrangements with them directly.

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

Inventory the Records Before Anyone Asks You to Send Them

Prepare a list of the documents and evidence that exist, who holds each one and what handling restrictions apply. An inventory is all the initial inquiry requires; the records themselves move later, through a channel agreed for that purpose. Record the open items, the approximate currency and the known changes against each item. An older diagram remains useful with its date and coverage stated, and it is presented as the current configuration once someone has verified it against the equipment on the pier.

The records an assessment draws on are the asset inventory with its owner column, the architecture drawings and responsibility records, the firewall and gateway rule exports with their dates, the identity directory groups that grant operational access, the vendor support contracts and the remote access approvals and revocations, the existing assessments and action registers with evidence of corrective work, the backup inventory with the record of the last actual restore, the software and licensing dependencies for the terminal operating system and the control networks, and the logging, time source and incident preservation procedures the facility relies on. The examiner reads the restore record before the backup policy and the revocation list before the access policy, because those two records are where the examiner looks to see how the paper is followed in practice.

Three items reward early attention: reconciling the vendor remote access list against the gateway configuration, extending the asset inventory from the IT estate out to the yard, and confirming that the incident contact named in the security plan is current. Listing any of these on the inventory is the first corrective action, and preparation is the best place to find them.

Bring the inventory and the diagram as they are, with their dates; the scoping call works from what exists.

Set the Operating Safeguards Before Any Active Method Is Proposed

Operations and engineering identify the sensitive equipment, the maintenance windows, the excluded techniques, the stop conditions and the recovery arrangements, and define the communication path if an unexpected condition occurs. For a terminal that means the crane and vehicle control networks, the vessel systems alongside, the gate during peak hours and anything that feeds a safety function; for a vessel it means propulsion, steering, navigation and cargo systems. These decisions belong to the people who run the terminal or the vessel, and the assessment team works within them and writes them into the method.

Existing records, interviews, configuration review and approved passive evidence are where the examiner looks first, with every live system left running as it is, and a competent examiner works through them fully before proposing anything active. Each active validation proceeds under its own written approval of its exact target, method, tool version, timing and operating conditions, with a named stop authority reachable during the window. Where a concern is better settled away from production, a representative or laboratory system is the right place for it, and the report states the differences between that system and the installed one. The rules of engagement that work are written with the terminal and read by the people who run it, alongside the corporate signature.

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

Agree How Security Plans and Other Sensitive Material Will Move

Security plans, detailed architecture, credentials and incident evidence belong in an approved controlled exchange. Identify the access restrictions, the intended recipients, the retention requirements and the rules for sharing information with vendors or other advisers before any of it is requested, and decide how Sensitive Security Information will be marked, stored and returned. The examiner expects to sign for those records and to hand them back or destroy them on an agreed schedule, and expects you to ask.

Keep the public inquiry to general facility information, your role and the decision you need to support. We arrange a secure exchange for Sensitive Security Information, plan excerpts, credentials and network drawings after the first call.

The controlled exchange is agreed on the first call; until then, describe only the facility, your role and the decision.

Define the Outputs and What Finished Means

Define the systems and questions covered, the methods, the exclusions, the deliverables, the review process and the client responsibilities. Distinguish the executive summary from the restricted technical evidence, and decide who owns each corrective action before the first finding is written, because an action register with an owner on every line is what turns a maritime assessment into change.

Completion means that the agreed work and review are finished, with the scope of the conclusions stated. The report describes what was examined and found within that scope, approval of a plan remains with the Coast Guard, and the report says so in its own words so every reader takes it the same way.

Expect the written output to include the scope and agreed operating conditions, evidence supported findings with their scope and priorities, corrective action ownership and verification criteria, management and technical readouts, and defined follow up work wherever additional validation is needed. The deliverables preview shows how those pieces fit together in the report your facility will receive.

Start With a Scope Conversation Using General Details

Describe the facility or vessel type, the general location, your role and the assessment question. Mention the work that already exists and the people available to define the operating boundaries. A senior practitioner will discuss the technical scope, the responsibilities and the handling arrangements for any later evidence exchange, and the first consultation is free.

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

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

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

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