# The Cybersecurity Officer Problem

Subpart F's Hardest Requirement for Small Maritime Operators

David W. Koran

*CyberAB Registered Practitioner Advanced*

*ISO/IEC 27001 Auditor and Implementer*

July 2026

# The Requirement Everyone Reads Past

The Coast Guard's Cybersecurity in the Marine Transportation System rule, codified at 33 CFR Part 101, Subpart F, is usually discussed in terms of its documents. The Cybersecurity Plan is due by July 16, 2027. The Cybersecurity Assessment must precede it. Training came due in January 2026 and recurs annually. Each of these obligations has a deadline, a deliverable, and a market of providers willing to help produce it.

One requirement in the rule does not fit that pattern. Under 33 CFR 101.630, each covered owner or operator must designate a Cybersecurity Officer, in writing, by name and title. Under 33 CFR 101.625, that named person must be accessible to the Coast Guard 24 hours a day, 7 days a week, and carries a list of duties that together amount to the standing management of the entire cybersecurity program. The CySO is not a document. The CySO is a person, and for most of the covered population, identifying that person is the hardest question the rule asks.

This paper examines why. It reviews the requirement as written, quantifies the workload the role carries, explains why the burden falls disproportionately on small operators, and evaluates the three staffing structures available to an owner or operator who must put a name on the line. It closes with the questions a management team should answer before designating anyone.

# The Requirement as Written

The regulatory text is short and specific. The owner or operator must designate a CySO in writing, by name and title, and the designation appears in the Cybersecurity Plan the Coast Guard reviews. The rule permits one individual to serve as CySO for more than one vessel, facility, or Outer Continental Shelf facility, and it permits the role to be assigned to a person who holds other responsibilities in the organization, provided the person can perform the duties of the position.

Those duties, enumerated at 33 CFR 101.625, define the job. The CySO must ensure that the Cybersecurity Assessment is conducted as required; that the cybersecurity measures in the Cybersecurity Plan are developed, implemented, and operating as intended; that an annual audit of the plan and its implementation is conducted, with the plan updated where the audit shows it no longer matches the operation; that the Cyber Incident Response Plan is executed and exercised; that the Cybersecurity Plan is exercised in accordance with 33 CFR 101.635; that cybersecurity inspections are arranged, whether standing alone or in conjunction with scheduled Coast Guard inspections; that problems identified by exercises, audits, or inspections are promptly corrected; that the cybersecurity awareness and vigilance of personnel is maintained; that personnel are

adequately trained; that all reportable cyber incidents are recorded and reported; and that cybersecurity drills and exercises are conducted and assessed.

Two features of the text deserve emphasis. First, the accessibility standard is continuous. The CySO must be reachable by the Coast Guard at any hour, which makes the designation an operational commitment rather than an organizational chart entry. Second, the verbs are supervisory but the accountability is personal. The rule does not require the CySO to perform every task with their own hands. It requires the CySO to ensure that each one happens, and when the Coast Guard examines the program, the CySO is the person answering by name.

The role also carries the single most consequential judgment in the rule. The definition of Critical Information Technology and Operational Technology systems at 33 CFR 101.615 turns on which systems, if compromised or exploited, could result in a transportation security incident, as determined by the CySO in the Cybersecurity Plan. The strictest measures in the rule, including executable code restrictions, protected and tested backups, and the patching of known exploited vulnerabilities without delay, attach to the systems the CySO designates. Whoever holds the role decides where the heaviest obligations in the regulation apply, and must be able to defend that decision on review.

# The Workload, Measured in Calendar Terms

The duties read quickly. Converted into an operating calendar, they describe a substantial standing workload. The recurring structure of Subpart F assigns the CySO responsibility for an annual Cybersecurity Assessment, an annual audit of the plan and its implementation, annual training for all personnel with access to covered systems, an annual exercise of the full program, and cybersecurity drills at least twice each calendar year, with successive drills expected to test different elements of the plan.

Between those scheduled obligations run the continuous ones. Reportable cyber incidents must be reported to the National Response Center whenever they occur. Known exploited vulnerabilities in Critical IT and OT systems must be patched, or compensating controls documented, without delay, which means the obligation arrives on the adversary's schedule rather than the operator's. New personnel must be trained within 5 days of gaining system access and no later than 30 days after hiring, a clock that runs constantly in operations with seasonal crews and routine turnover. Records of all of it, training rosters, drill and exercise documentation, audit findings, incident reports, and correction records, must be maintained and producible, and the Cybersecurity Plan itself is sensitive security information protected under 49 CFR part 1520.

On top of the recurring cycle sits the five-year plan renewal, which carries a penetration test and a certification letter listing all identified vulnerabilities. The renewal is assembled from the records the annual cycles produced, which means the quality of the CySO's year-to-year administration determines whether the renewal is an assembly exercise or a reconstruction project.

A reasonable planning estimate for a single small facility or a modest fleet places the role at a meaningful fraction of a working year: the annual assessment and audit each consume focused weeks rather than days when done honestly, the training, drill, and exercise cycle requires design and documentation rather than mere occurrence, and the continuous obligations impose an availability cost that does not appear on any schedule. The role is smaller than a full-time position in most small operations and much larger than a collateral duty performed in spare hours. That awkward size is the heart of the problem.

# Why the Burden Falls on the Smallest Operators

In the regulatory analysis accompanying the final rule, the Coast Guard estimated the affected population at 3,447 owners and operators, and determined that approximately 3,130 of them, roughly 91 percent, are small entities. The rule was written with that population in view, and the Coast Guard declined during the rulemaking to exclude operators with limited information technology footprints, reasoning that even minimal connected systems can expose positional data, personal information, or operational access.

For the large operators in the remaining 9 percent, the CySO requirement is an assignment problem. A company with a security department selects a qualified individual, adjusts a job description, and moves on. For the small majority, the requirement is a genuine dilemma. A typical covered small entity, a family-held terminal, a towing company running a handful of vessels, an offshore service operator, employs no one whose background spans cybersecurity, maritime operations, and regulatory administration. The office manager who handles the Facility Security Officer paperwork does not have the technical depth the Critical IT and OT determination requires. The managed service provider who maintains the computers does not know the vessels, is not an employee, and is not accessible to the Coast Guard at 3 a.m. The owner has the authority and the operational knowledge but not the time or the technical grounding.

The market compounds the difficulty. Cybersecurity professionals are expensive and scarce, and the subset with maritime operational context is smaller still. A small

operator cannot justify a full-time hire for a role that is a fraction of a position, cannot credibly upskill an existing employee by the deadline without support, and cannot simply hand the title to the least unwilling manager without accepting that the program will be carried in name only. Every option available inside the organization involves a compromise, and the compromises are exactly what a Coast Guard review is structured to find.

# Three Structures, Each with a Price

In practice, a covered operator has three ways to fill the role, and each carries tradeoffs that deserve to be stated plainly.

The first structure is internal designation with external support. An existing employee, often the FSO, an operations manager, or an owner, takes the designation, and the organization buys the technical depth around them: support for the assessment, help with the Critical IT and OT determination, training design, and periodic advisory access. The strengths of this structure are real. The CySO knows the operation, is present in it daily, and satisfies the accessibility standard naturally. The price is the development burden on the designee, who must grow into the technical dimensions of the role, and the risk that the day job crowds out the program between deadlines. This structure works where the designee has genuine capacity and management treats the supporting relationship as permanent rather than as a one-time purchase.

The second structure is the shared CySO. The rule expressly permits one individual to serve multiple vessels, facilities, or OCS facilities, and for fleet operators and multi-site companies this consolidation is often the only economically rational design. Its strength is concentration: one qualified person, developed or hired once, amortized across the operation. Its price is the same concentration. The shared CySO's calendar multiplies with each covered asset, the 24/7 accessibility standard does not divide, and a single departure removes the program's institutional memory from every vessel and facility at once. This structure works where the covered assets are genuinely similar and the organization plans deliberately for succession.

The third structure is the outside designee, a contracted individual who takes the designation by name. The strengths are immediacy and depth: the role is filled at once by someone who does this work continually, across operations, with the regulatory and technical grounding the position demands. The prices are equally real and should not be minimized by anyone offering the service. An outside CySO does not live in the operation, and must build and continually refresh the operational knowledge an internal designee has by default. The accountability the rule creates cannot be transferred along with the title; the owner or operator remains responsible for the program, and a

contracted designee adds a relationship to manage rather than removing one. The arrangement also depends on contractual clarity about accessibility, incident response, records custody, and what happens when the relationship ends, because a program whose records and memory leave with a vendor was never the operator's program. This structure works where the operator lacks any credible internal candidate, treats the outside designee as embedded rather than remote, and writes the exit provisions before signing.

No structure is free, and the correct choice is a function of the operation rather than a general rule. What all three share is a dependency the rule quietly imposes: whoever holds the title, the organization around them must supply time, access, records, and management attention. A CySO of any kind, internal, shared, or contracted, fails in an organization that treats the designation as the end of its involvement.

# Questions to Answer Before Designating Anyone

An owner or operator approaching the designation decision can test any candidate structure against a short set of questions. Who, by name, will the Coast Guard reach at any hour, and does that person know it? Who will make and defend the Critical IT and OT determination, and do they understand both the systems and the transportation security incident standard well enough to do so? Who owns the annual calendar, the assessment, the audit, the training cycle, the drills, and the exercise, and where does that time come from? Where do the records live, who maintains them, and would they survive the departure of the person who holds the role today? What does the arrangement cost per year, honestly counted, including the internal time no invoice captures? And if the designated person left in six months, what would remain?

A structure that produces confident answers to those questions will support the program the rule requires. A structure that cannot answer them will produce a name in a plan, which is what the requirement asks for on paper and precisely what it was written to prevent in practice.

# Conclusion

The deadlines in Subpart F point at documents, and documents can be bought. The Cybersecurity Officer requirement points at a person, and for the small operators who make up nine-tenths of the covered population, that person does not currently exist inside the organization. The operators who handle this requirement well will be the ones who treat the designation as a staffing decision with a multi-year horizon, made

deliberately among the three available structures, rather than as a blank on a form filled in during the final weeks before submission. The plan will be reviewed once. The name in it will answer for the program every year afterward.

# About the Author

David W. Koran advises covered vessel and facility operators on cybersecurity readiness under 33 CFR Part 101, Subpart F, work he conducts onsite in the operating environment. He holds the CyberAB Registered Practitioner Advanced (RPA) credential and ISO/IEC 27001 certifications as an auditor and implementer, and is the founder of a consulting practice serving Defense Industrial Base contractors and their legal counsel, including maritime operators in shipbuilding, repair, and logistics, with a focus on readiness, enablement, and implementation. He is the author of Cybersecurity in the Marine Transportation System. He can be reached at dkoran@davidkoran.com or (802) 335-2662.

# References

33 CFR Part 101, Subpart F, Cybersecurity, including § 101.615 (definitions), § 101.620 (owner or operator responsibilities), § 101.625 (Cybersecurity Officer), § 101.630 (Cybersecurity Plan and training), § 101.635 (drills and exercises), and § 101.650 (cybersecurity measures). Electronic Code of Federal Regulations: https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F

Cybersecurity in the Marine Transportation System, Final Rule, 90 FR 6298, January 17, 2025, including the regulatory analysis of the affected population and small entities. Federal Register: https://www.federalregister.gov/documents/2025/01/17/2025-00708/cybersecurity-in-the-marine-transportation-system

U.S. Coast Guard, additional policy and guidance in support of 33 CFR Part 101, Subpart F, including CG-5PC Policy Letter 01-26, Cybersecurity Assessment Initial Scoping and Process, announced June 4, 2026. Maritime Commons: https://www.news.uscg.mil/maritime-commons/Article/4512023/us-coast-guard-releases-additional-policy-and-guidance-in-support-of-33-code-of/

U.S. Coast Guard Maritime Industry Cybersecurity Resource Center, implementation guidance and FAQ materials: https://www.uscg.mil/MaritimeCyber/