Cydome Unveils Cyber-Incident Reporting Tool as the U.S. Maritime Sector Faces Law Enforcement

A new tool provides immediate compliance support as maritime operators become federally required to report cyber incidents under U.S. law

From Cydome, July 28, 2025

Tel Aviv, July 28, 2025 – With Federal maritime cybersecurity reporting rules that entered enforcement on July 16, U.S.-bound maritime operators are now federally required to report cyber incidents, marking a turning point for shipowners, operators, and offshore stakeholders. In response, Cydome, a leading provider of class-endorsed maritime cybersecurity solutions, has launched a free reporting tool to simplify compliance. By simply registering, operators take an immediate first step toward meeting the Coast Guard's cyber-reporting expectations.

Cydome data shows that roughly every three days, a shipping company faces a cyber threat, yet many still struggle to operationalise existing guidance. The new U.S. regulation, applying to vessels, facilities, terminals, and outer continental shelf (OCS) facilities, mandates not only incident reporting, but also cybersecurity staffing, procedures, and governance. Incident reporting is just one pillar of the revamped Federal Law.

Many of the incidents now deemed reportable are everyday glitches, such as GPS spoofing or jamming, short VSAT dropouts, partial software updates that require a system restart, or an unauthorized USB stick being plugged into a bridge computer; a sustained loss or degradation of communications (e.g., satellite, VHF, or navigation-data links), or a series of mistyped passwords that lock an account, can also trigger a mandatory report. Taken together, these otherwise routine events can generate dozens of mandatory reports during a single voyage. Non-compliance is costly: the Coast Guard may impose substantial civil fines, suspend a vessel's certificate, detain the ship in port, or issue Captain of the Port orders that require anchorage, tug escort, or a full halt to cargo operations until the vulnerability is remedied.

Cydome's digital platform provides a step-by-step incident workflow, complete with built-in U.S. Coast Guard templates that are pre-filled and auto-routed for seamless submission. The tool enables internal escalation, from IT to CISO to senior management, as well as formal reporting to regulators, helping companies stay compliant efficiently, automatically, and securely. It is built to accommodate both large organizations with dedicated IT or cyber teams and companies with more limited in-house capabilities. It is designed for the operational realities of multi-class fleets, where vessels may fall under different standards and reporting chains.

"This tool puts operators back in control," said Nir Ayalon, CEO and Founder of Cydome. "We designed it to be simple enough for maritime companies, yet powerful enough to deliver a full audit trail for inspectors. With enforcement now real, the sector needs a no-obstacle solution, and we're proud to deliver exactly that."

While the U.S. Coast Guard has been tasked to begin enforcing the new cyber-reporting legislation, Cydome turns the cyber-incident ensuring process into a few clicks. The platform mirrors the Coast Guard's forms, auto-fills every required field, timestamps supporting evidence, and routes each report from shipboard IT through the CISO and senior management directly to the National Response Center (NRC). In moments, crews can file an inspector-ready record for navigation, propulsion, ballast, and other critical IT or OT systems, long before an audit team arrives.

With U.S. enforcement already underway, compliance urgency is high. At the same time, the EU's NIS2 directive has taken effect and will soon be actively enforced. Cydome's class-endorsed, independent platform gives European operators the same streamlined reporting workflow, automated escalation paths, and regulator-ready templates that U.S. users already rely on. By design, the tool adapts seamlessly to multiple

regulators, classification societies, and standards, giving mixed fleets a single, simple route to full compliance on both sides of the Atlantic.

“Policy alone won’t keep ships safe; crews need a clear, repeatable way to act,” said Dr. Gary Kessler, former cyber official at the U.S. Coast Guard and a leading voice in maritime cybersecurity. “By translating every Coast Guard requirement into a straightforward process, Cydome delivers that clarity, and because the solution is class-endorsed, the same disciplined approach works across multi-class fleets and the new European rules as well.”

About Cydome

Cydome is a class-certified cybersecurity pioneer, purpose-built for maritime and critical infrastructure. Trusted by all major classification societies for its independence, Cydome’s ISO-certified platform secures IT, OT, and onboard communications, automates vulnerability management, and simplifies compliance with US Coast Guard, NIS2, and global regulations. With seamless onboard deployment and centralized control, Cydome empowers operators to detect, respond to, and protect against cyber threats, ensuring vessels remain secure and compliant.