Seatrade Maritime NEWS

Shipping concerned over onerous new US cyber-security regulations

Industry feedback on new cyber-security regulations for US flagged vessels is critical of the level of burden, the practicality of implementation, and lack of alignment to existing measures.

Barry Parker | May 23, 2024

In late February, the United States Coast Guard (USCG) issued a Notice of Proposed Rulemaking (NPRM) regarding cyber security for US flagged vessels. More formally, the proposed changes to Federal Regulations are described as an action to: “update maritime security regulations by adding regulations specifically focused on establishing minimum cybersecurity requirements for US-flagged vessels, facilities on the Outer Continental Shelf, and US facilities subject to regulations under the Maritime Transportation Security Act of 2002.”

When NPRM's are issued, comments from affected parties are solicited; the comment period has now expired, and responses will then be considered before the final wording of the new regulations is put in place.

The proposed wording of the new regulatory language is lengthy, building on the USCG observation that: "The maritime industry is undergoing a significant transformation that involves increased use of cyber-connected systems. While these systems improve commercial vessel and port facility operations, they also bring a new set of challenges affecting design, operations, safety, security, training, and the workforce."

Referring to a Spring 2021 cyber-hack of the Colonial Pipeline-connecting the US Gulf region to the Northeast, which led to temporary waivers of the Jones Act to allow coastwise moves of petroleum products), the USCG opines in its NPRM, that: "Every day, malicious actors (including, but not limited to, individuals, groups, and adversary nations posing a threat) attempt unauthorised access to control system devices or networks using various communication channels."

Dozens of comments have come in from industry. At a very practical level, smaller companies, such as those in the coastwise or inland river tug and barge trades do not have large Information Technology (IT) departments, and often hire external consultants to assist in cyber-related matters. In the NPRM responses, a number of tug operators including Florida Maritime Transportation, Western Towboat Company, Dann Marine Towing, Golding Barge Lines and Andrie (members of American Waterway Operators, or AWO- which possibly recommended the wording for its members to respond individually) expressed the following concerns:

- Develop risk-based plans with applicability scaled to the companies' actual business profile
- Add cybersecurity to Alternative Security Plans filed by members of AWO (and other groups)

- Streamline incident reporting through the National Response Center and set thresholds for reportable incidents
- Rethink the role of cyber-security officers (not practical to have aboard every vessel)
- Reduce the frequency of proposed cybersecurity drills

Maersk Line, which has a significant presence in US flag non-Jones Act (foreign) trades, offered a crafted commentary touching on similar points (but going into great detail), noting that: “We consider this a significant step toward enhancing the cybersecurity posture of this critical infrastructure sector. However, to maximize its impact and feasibility, we recommend further enhancements in the areas of clarity, efficiency, and alignment with existing programs.”

They thought that the USCG objectives could be met by providing “clear, standardised, risk-based, and practical measures that leverage existing industry best practices and avoid creating undue burdens.”

In another company-crafted response, Liberty Global Logistics, LGL, also operating US flag vessels in the international realm, suggested that “the regulations as proposed are extremely onerous, financially burdensome, and impractical in terms of timelines and ultimate implementation.”

On the subject of ransom-ware attacks (a major motivation for cyber-attacks), LGL said: “A company’s decision as to how to respond to a ransomware attack is its own subjective prerogative and if a company opts to pay a ransom, it should not be required to report that information, as the very act requiring reporting may ultimately discourage certain companies from making ransom payments, which may actually increase the overall number of cyber incidents and ransomware attacks.”

Resources:
The NPRM can be downloaded here: https://www.regulations.gov/document/USCG-2022-0802-0001

The industry comments mentioned in the article (as well as other responses) can be found at: https://www.regulations.gov/document/USCG-2022-0802-0001/comment

---