



MARITIME CYBER RISK MANAGEMENT

Technical Notice SLS.34

*Notice to Shipowners, Ship Operators, Managers, Masters,
Owners' Representatives and Recognised Organisations*

The Directorate reminds all concerned to the provisions contained in IMO Resolution [MSC.428\(98\)](#) concerning Maritime Cyber Risk Management in Safety Management Systems. Inter alia, the IMO Resolution encourages ship management companies to ensure that cyber risks are appropriately addressed in the vessel's safety management systems (SMS) with regards to their operations both ashore and aboard, by no later than the first annual verification of the Document of Compliance (DOC) after 1 January 2021.

Recognizing the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement, it has been noted that some of the most vulnerable systems, include amongst others:

Bridge systems,
Cargo handling and management systems,
Propulsion and machinery management and power control systems,
Access control systems,
Passenger servicing and management systems,
Passenger facing public networks,
Administrative and crew welfare systems,
Communication systems.

Notwithstanding the fact that the said Resolution is non-mandatory, the attention of all stakeholders is drawn to the fact that, some countries like the US have made such a requirement mandatory to all vessels that call on ports in the U.S. regardless of the ship's flag.

Accordingly, if objective evidence is identified indicating that the foreign flagged vessel calling at US ports failed to implement its SMS with respect to cyber risk management, the following actions would be directed by the PSCO:

- 1) Should cyber risk management has not been incorporated into the vessel's SMS by the company's first annual verification of the DOC after January 1, 2021, a deficiency should be issued with action code 30 - Ship Detained.
- 2) Should objective evidence indicate that the vessel failed to implement its SMS with respect to cyber risk management, a deficiency for both the operational deficiency and an ISM deficiency would be issued with an action code 17 - Rectify Prior to Departure or an action code 30 – Ship Detained depending on its seriousness.



It is imperative that owners/managers ensure that their crews are familiar with the requirements in force in their trading areas.

Furthermore, it is strongly recommended that since the regulatory enforcement strategy may differ from one region/port to another, crews must be provided with clear procedures and guidance on this matter well in advance of the vessel's intended area of operation and port of call.

To this effect, it is recommended that ship managers of Maltese registered ships undertake the necessary actions to ensure that the systems are in compliance with requirements in force in their trading areas. This should be done at the earliest opportunity to avoid the risk of detention or unnecessary delays.

Merchant Shipping Directorate

30 December 2020