सत्यमेव जयते
भारत सरकार / GOVERNMENT OF INDIA
पत्तन, पोत परिवहन और जलमार्ग मंत्रालय
MINISTRY OF PORTS, SHIPPING AND WATERWAYS
समुद्रीय प्रशासन महानिदेशालय, मुंबई
DIRECTORATE GENERAL OF MARITIME ADMINISTRATION, MUMBAI

File No. 25-59011/1/2023- MSB **Date: 04.08.2026**

DGMA Circular No. 46 of 2026

Subject: Maritime Cyber Security Risk Management for Port Facilities under the International Ship and Port Facility Security (ISPS) Code – reg.

Sir,

The International Ship and Port Facility Security (ISPS) Code aims to establish appropriate measures to prevent security incidents affecting ships and port facilities. With increasing digitalization and automation of port operations, cyber threats have emerged as a potential source of security incidents affecting port facilities and maritime operations.

2. Modern port facilities increasingly rely on Information Technology (IT) and Operational Technology (OT) systems, including terminal operating systems, cargo handling systems, vessel traffic management systems, access control systems, surveillance systems, communication networks and other interconnected digital infrastructure. Compromise of such systems through cyber incidents may adversely affect the safety, security and continuity of port operations.

3. Cyber threats to port facilities may arise from unauthorized access, malware, ransomware, phishing, remote access vulnerabilities, third-party access and compromise of interconnected systems. Such threats may impact the confidentiality, integrity and availability of critical systems and information.

4. Port Facilities may consider incorporating cyber security risk assessment as part of the Port Facility Security Assessment (PFSA). Such assessment may identify critical cyber assets, cyber vulnerabilities, threat vectors and potential impacts on port security and operations. Port Facilities may also undertake periodic vulnerability assessments of critical information systems and ensure timely remediation of identified vulnerabilities.

5. Particular consideration may be given to cyber risks associated with access control and identification systems, CCTV and surveillance systems, cargo and terminal operating systems, vessel

traffic and communication systems, remote access arrangements, third-party service providers and vendors, and data storage and network infrastructure. Appropriate measures may also be considered for segregation and protection of Information Technology (IT) and Operational Technology (OT) environments supporting port operations. Cyber security requirements may be considered while engaging third-party service providers, vendors, contractors and personnel having access to critical systems and networks.

6. Appropriate mitigation measures identified through the assessment may be incorporated, as applicable, within the Port Facility Security Plan (PFSP) and related security procedures. Such measures may include access controls, network protection, incident response procedures, backup and recovery arrangements, business continuity measures and protection of personal data, wherever applicable. Port Facilities may periodically test backup, recovery and business continuity arrangements to enhance resilience against cyber incidents and operational disruptions.

7. Port Facility Security Officers (PFSO) and other personnel having security responsibilities should possess adequate awareness of cyber security risks relevant to port operations. Port Facilities may designate a suitable officer or function responsible for overseeing cyber security risk management, coordination and compliance activities. Port Facilities are encouraged to conduct periodic cyber security awareness programmes, familiarization sessions, drills, exercises and simulations to assess preparedness and response effectiveness.

8. Port Facilities may establish suitable procedures for cyber incident reporting, response, containment and recovery to minimize disruption of critical operations. Cyber security measures should be periodically reviewed and updated considering evolving threats, technological developments and operational requirements.

9. Port Facilities may refer to the Cybersecurity Guidelines for Ports and Port Facilities issued by International Association of Ports and Harbours (LAPH), IMO Resolution MSC.428(98), MSC-FAL.1/Circ.3 and Maritime Cybersecurity Assessment Guide issued by the security agencies involved in cyber security guidance while strengthening cyber security preparedness under the ISPS framework.

10. The present framework for cyber security and data protection as codified and deployed in the DGS Office order 133/2025 dated 21.11.2025 wherein the Chief Information Security official's role is critical and similar institutional mechanism in all port facilities are strongly advocated for compliance and pre-emptive cyber security measures and certification / audit thereof.

This is issued with the approval of the Competent Authority.

(Capt. Nitin Mukesh)

Dy. Nautical Advisor-cum Senior DDG (Tech)