
THE ISPS CODE, PORT SECURITY AND SEAFARER PROTECTION: A CRITICAL LEGAL ANALYSIS OF FLAG STATE, PORT STATE AND LABOUR-SUPPLYING STATE RESPONSIBILITIES IN INDIA

Anjana Ajayan, LL.M. (Maritime Law),
Bharata Mata School of Legal Studies, Aluva, Kerala, India

ABSTRACT

The International Ship and Port Facility Security (ISPS) Code, given mandatory effect through Chapter XI2 of the International Convention for the Safety of Life at Sea (SOLAS), constitutes the principal international framework for the security of ships and port facilities. Although the Code is principally directed towards preventing unlawful interference, its implementation occurs within a workplace in which seafarers, port workers, shipowners, port authorities and public agencies interact. This article examines the relationship between maritime security and maritime labour, with particular emphasis on the allocation of responsibilities among flag States, port States and labour-supplying States. It analyses the legal structure and operational mechanisms of the ISPS Code, including security assessments, security plans, security levels, designated security officers, access control, ship security alerts, declarations of security, drills, audits and verification. It then examines the complementary role of the Maritime Labour Convention, 2006, the STCW Convention, the ISM Code and UNCLOS. The article also evaluates India's contemporary statutory framework under the Merchant Shipping Act, 2025 and the Indian Ports Act, 2025. It argues that maritime security and seafarer protection should be implemented as interconnected elements of maritime governance. Effective regulation requires risk-based decision-making, proportionate restrictions, competent inspection, inter-agency coordination, meaningful training, cybersecurity preparedness and protection of essential welfare and employment interests during heightened security conditions.

Keywords: ISPS Code; maritime security; port security; SOLAS; seafarers; Maritime Labour Convention; flag State; port State control; labour-supplying State; Merchant Shipping Act, 2025; Indian Ports Act, 2025.

LIST OF ABBREVIATIONS

IMO – International Maritime Organization

ILO – International Labour Organization

ISPS Code – International Ship and Port Facility Security Code

SOLAS – International Convention for the Safety of Life at Sea, 1974

MLC, 2006 – Maritime Labour Convention, 2006

STCW – International Convention on Standards of Training, Certification and Watchkeeping for Seafarers

ISM Code – International Safety Management Code

PFSO – Port Facility Security Officer

SSO – Ship Security Officer

CSO – Company Security Officer

PSC – Port State Control

UNCLOS – United Nations Convention on the Law of the Sea

1. INTRODUCTION

The security of ships and port facilities has a direct relationship with the protection of maritime workers. Seafarers are not merely occupants of ships; they are essential participants in the implementation of security measures. They control access to the vessel, maintain watchkeeping systems, respond to suspicious activities and participate in emergency drills. Consequently, a security regime that ignores labour conditions may be ineffective in practice. Fatigue, inadequate training and poor communication can reduce the ability of a crew to respond to a security incident. Maritime security law must therefore be examined together with marine employment and labour standards.

The legal importance of the ISPS Code is that it establishes a structured system of preventive security. It requires States and maritime actors to identify threats, assess vulnerabilities and implement measures corresponding to the risk. The framework is not intended to impose identical measures at every port. Instead, it permits security arrangements to reflect local circumstances while maintaining an internationally recognised minimum. This flexibility is especially important for busy commercial ports where excessive controls could disrupt trade and interfere with legitimate work.

This article consequently adopts an integrated approach. It examines the ISPS Code and its relationship with SOLAS, the MLC, 2006, STCW, the ISM Code and UNCLOS, and then considers India's current statutory framework. The central issue is whether maritime security

can be implemented effectively without undermining the lawful interests and welfare of seafarers. The analysis suggests that security and labour protection are not competing objectives when regulation is based on risk assessment, proportionality, professional training and clear allocation of responsibility.

A further legal consideration is the position of the seafarer as a worker operating inside a securityregulated workplace. Security measures are legitimate only when they have a legal basis and are applied through established procedures. A port facility cannot achieve genuine security by disregarding the human element. Crew members possess operational knowledge of the vessel and may be the first persons to detect an unusual event. Their participation should therefore be encouraged through reporting systems, training and consultation. The security regime is strongest when the crew understands the reasons for controls and can distinguish a genuine security requirement from an arbitrary restriction.

2. RESEARCH OBJECTIVES, SCOPE AND METHODOLOGY

The study has five principal objectives. First, it explains the legal foundation and operational structure of the ISPS Code. Secondly, it analyses the responsibilities of ships, shipping companies, port facilities and Governments. Thirdly, it examines the relationship between maritime security and marine employment, particularly the responsibilities of flag States, port States and laboursupplying States. Fourthly, it evaluates the Indian legal framework following the enactment of the Merchant Shipping Act, 2025 and the Indian Ports Act, 2025. Finally, it identifies implementation challenges and proposes measures for strengthening compliance.

The scope is deliberately limited to maritime security, port safety and the State responsibilities relevant to marine employment and labour. The study concentrates on the ISPS Code, SOLAS Chapter XI-2, maritime labour standards, flag State control, port State control, labour-supplying State responsibilities and the corresponding Indian legal framework. This keeps the assignment closely aligned with the subject under examination.

The research method is doctrinal and analytical. Primary materials include SOLAS Chapter XI-2, the ISPS Code, the MLC, 2006, STCW, the ISM Code, UNCLOS and relevant Indian statutes. Secondary materials include IMO and ILO guidance, official maritime administration publications and scholarly commentary. The analysis compares the allocation of responsibilities under international instruments with the institutional framework in India. The

study also uses a rightsoriented perspective to assess whether security measures remain necessary, proportionate and compatible with seafarers' welfare.

The analytical framework also distinguishes three questions: what international law requires, how India implements those obligations, and whether implementation is effective in practice. A doctrinal study can identify gaps between treaty standards and domestic legislation, but it must also examine institutional capacity. The article therefore evaluates not only legal provisions but also the functions of inspectors, port authorities, security officers and maritime administrators.

3. EVOLUTION AND DEVELOPMENT OF THE ISPS CODE

The development of the ISPS Code represents a significant change in the philosophy of international maritime regulation. Traditional maritime conventions concentrated mainly on accidental risks to life, such as collision, fire, structural failure and navigational error. Deliberate acts presented a different category of risk because they could be planned, concealed and directed at the vulnerabilities of ships or ports. The international community therefore required a framework capable of preventing unlawful interference before an incident occurred.

The diplomatic conference held in December 2002 adopted amendments to SOLAS and introduced Chapter XI-2. The ISPS Code was developed as the practical instrument supporting those amendments. It entered into force on 1 July 2004, only eighteen months after adoption. The speed of implementation demonstrates the importance attributed to maritime security. The Code is now the principal mandatory international framework for ship and port facility security under IMO instruments.

Its evolution also reflects a movement from static regulation towards risk management. Instead of prescribing every physical security measure in advance, the Code requires assessment of threats and vulnerabilities and then permits measures appropriate to the assessed risk. This model has allowed the framework to respond to changing threats, although it also creates challenges because effective implementation depends on the quality of national administration, assessments, audits and professional judgement.

The historical significance of the Code is also institutional. It required maritime administrations to develop security authorities and procedures that had not previously existed in the same form.

Ports had to move towards formal security assessments and approved plans, while companies had to designate security officers and establish shipboard systems. The result was a stronger culture of preventive security. At the same time, rapid implementation created differences in administrative capacity among States. Continued IMO guidance, training and audits have therefore remained important for achieving consistent implementation.

4. LEGAL BASIS AND STRUCTURE OF THE ISPS CODE

The ISPS Code derives its mandatory legal effect from SOLAS Chapter XI-2. Regulation XI-2/3 requires Contracting Governments to give effect to the Code. The Code itself is divided into Part A and Part B. Part A contains mandatory requirements, whereas Part B provides guidance for implementing those requirements. The distinction is important in legal analysis because Part A forms part of the mandatory SOLAS security framework while Part B primarily assists States and industry in understanding and applying the mandatory provisions.

The structure of the Code distributes responsibilities between the Contracting Government, the designated authority, companies, ships and port facilities. At government level, the State must establish the framework through which security assessments, security plans, certification and verification are administered. At company and ship level, security officers and the Master are given defined functions. At port level, the Port Facility Security Officer implements the approved security plan and coordinates with ships and relevant authorities.

This distribution is consistent with the principle of shared responsibility. Maritime security cannot be achieved by the port alone because ships carry their own security systems; nor can a ship protect itself if the surrounding port is vulnerable. The ISPS framework therefore creates a chain of responsibility extending from national policy to operational personnel. Legal accountability is strengthened when each participant knows what it must do and which authority has power to verify compliance.

The legal architecture illustrates the interaction between treaty law and technical standards. SOLAS supplies the binding international obligation, while the ISPS Code supplies detailed operational requirements. Domestic legislation then identifies competent authorities and enforcement powers. This layered structure allows technical rules to be updated without rewriting the entire domestic maritime statute, but it also requires administrators and courts to understand the relationship between treaty provisions, the Code and national rules. Where a

conflict appears, the applicable domestic legislation and international obligations must be interpreted carefully and consistently.

5. OBJECTIVES AND PRINCIPLES OF MARITIME SECURITY

The principal objective of the ISPS framework is to establish an international standard for detecting security threats and taking preventive measures against incidents affecting ships and port facilities. The framework seeks to establish a common methodology for security assessment, to exchange security-related information, to require security plans and to provide mechanisms for response when security levels change. The underlying principle is prevention through preparedness rather than reliance solely upon post-incident investigation.

Risk management is central to this objective. Security measures should correspond to the nature and seriousness of the threat. A port handling sensitive cargo or located in a high-risk environment may require stronger controls than a facility with a different risk profile. This does not mean that security is optional; it means that the measures used to fulfil mandatory obligations should be selected through reasoned assessment. Risk-based regulation also permits authorities to concentrate resources where they are most needed.

Another principle is cooperation. Maritime security involves public authorities, private shipping companies, terminal operators, port workers and seafarers. Information must move quickly between them, especially where a threat affects more than one facility or ship. Cooperation also extends internationally because ships move between jurisdictions. The success of the ISPS Code therefore depends on mutual confidence, consistent procedures and the willingness of States to share appropriate security information.

The preventive character of the regime means that authorities must make decisions before certainty about an incident exists. This inevitably involves judgement and uncertainty. Legal safeguards are therefore important. Security assessments should be based on credible information, measures should be documented and decisions should be capable of review. The principle of proportionality is particularly relevant to marine labour because security restrictions may affect working arrangements and access to shore. A credible system should protect the port without creating unnecessary interference with lawful maritime employment.

6. PORT SAFETY AND PORT FACILITY SECURITY REGIME

Port safety and port security are related but legally distinct concepts. Safety generally addresses accidental risks and the protection of life, property and the marine environment from operational hazards. Security addresses intentional unlawful acts such as terrorism, sabotage, unlawful entry, theft and other deliberate interference. The distinction helps allocate regulatory functions, but the two systems must operate together. A security breach can create a safety emergency, while an unsafe port environment can magnify the consequences of a deliberate attack.

The ISPS Code requires port facilities to identify security-sensitive areas and establish appropriate protective measures. These may include access control, monitoring, surveillance, cargo security, control of ship's stores and security communications. Port safety systems may simultaneously regulate navigation, dangerous goods, fire protection, occupational safety, emergency response and pollution prevention. The port authority therefore needs an integrated governance model in which security does not operate in isolation from ordinary port operations.

For marine employment, the combined regime is important because seafarers work in the interface between ship and port. They may be exposed to security threats while also being subject to occupational hazards. Security procedures should be designed so that emergency medical access, evacuation, fire response and other safety functions remain possible. The strongest legal approach is one that protects the ship, port, worker and public as parts of one interconnected system.

The integration of safety and security also has implications for emergency command. A fire, collision or hazardous-material incident may require one response structure, while an intentional attack may require another. Ports should avoid situations in which agencies compete for control or provide contradictory instructions. Joint exercises involving safety and security personnel can clarify command relationships. For seafarers, this is important because they may have to implement emergency procedures before shore-based responders arrive. Legal planning should therefore account for the first minutes of an incident, not merely the later investigation.

7. PORT FACILITY SECURITY ASSESSMENT

The Port Facility Security Assessment is the analytical foundation of the security plan. It should

identify important assets, infrastructure, access points and operational activities and consider how those elements could be exploited by a person seeking to cause harm. The assessment must consider both land-side and waterside approaches and should take account of cargo operations, passenger or crew movement, ship interfaces, restricted areas, communications and existing protective measures.

An assessment should be evidence-based rather than merely descriptive. Information from previous incidents, law-enforcement agencies, intelligence sources, port operators and shipowners may assist in identifying realistic threats. Vulnerabilities should be prioritised according to their potential consequences and likelihood. The purpose is not to eliminate every conceivable risk, which may be impossible, but to reduce significant risks to an acceptable level through proportionate protective measures.

The assessment must remain dynamic. Port infrastructure changes, new technologies are introduced, cargo patterns evolve and security threats change. A security assessment that accurately reflected conditions several years ago may no longer be sufficient. Periodic review and review following significant changes or security incidents are therefore essential. Seafarers and port workers should also be considered as human elements within the assessment because training, fatigue, communication and procedural errors can influence security outcomes.

A legally sound assessment should distinguish between vulnerability and threat. A vulnerable access point is not necessarily a high-risk point unless there is a credible threat capable of exploiting it. Conversely, a low-frequency threat may deserve significant attention if the potential consequences are catastrophic. This analytical distinction helps prevent both over-securitisation and under-protection. The assessment should also identify human vulnerabilities, including inadequate staffing, fatigue, poor communication and insufficient training. Security is ultimately implemented by people, and the assessment must account for their capacity to perform under pressure.

8. PORT FACILITY SECURITY PLAN

The Port Facility Security Plan is the operational document through which the results of the security assessment are implemented. It should set out the security measures to be followed at each applicable security level and identify the responsibilities of personnel. Typical areas include access control, restricted areas, surveillance, cargo handling, ship's stores,

communications, reporting of security incidents, emergency response and coordination with ships and authorities.

The plan should be practical rather than merely formal. Security personnel must be able to understand their duties quickly, particularly during an emergency. The plan should therefore establish clear lines of authority, communication methods and procedures for escalating a situation. It should also identify arrangements for drills and exercises and the process through which deficiencies are recorded and corrected. Confidentiality is important because detailed security information may itself be sensitive.

A port facility security plan should be coordinated with the ship security arrangements of vessels using the facility. The interface between ship and port is a point of particular vulnerability because cargo, personnel, stores and information move between them. Consistency of procedures can reduce confusion and delay. At the same time, security plans should provide for legitimate welfare and emergency needs of seafarers, including medical access and necessary movement under controlled conditions.

The security plan should also be connected with other port emergency plans. A port normally has procedures for fire, pollution, medical emergencies, evacuation and natural disasters. The security plan should explain how those arrangements interact when an event has both security and safety dimensions. Confidentiality is necessary, but excessive secrecy can prevent operational personnel from understanding their duties. The appropriate balance is controlled distribution of sensitive information combined with adequate training. Plans should be tested, reviewed and amended after exercises and actual incidents.

9. SECURITY LEVELS UNDER THE ISPS CODE

The three security levels are a central feature of the ISPS Code. Security Level 1 represents the normal minimum appropriate protective measures maintained at all times. Security Level 2 is a heightened level where there is an increased risk of a security incident and additional protective measures are required. Security Level 3 applies for a limited period when a security incident is probable or imminent and specific additional measures are required.

The graduated model avoids two extremes. Permanent application of the highest level would make ordinary maritime trade inefficient, while maintaining minimal measures during a serious

threat would be inadequate. The system instead permits security controls to be intensified according to circumstances. Ships and port facilities must be prepared to implement the measures associated with each level, and communication between the competent authority, port and ship is essential.

Higher security levels may affect crew movement, access to shore facilities, cargo operations and working arrangements. Such consequences should be managed through clear procedures. Restrictions on ordinary shore leave may sometimes be unavoidable during a serious security threat, but essential medical treatment and emergency movement should remain subject to appropriate arrangements. Security measures should be lawful, necessary and proportionate to the threat and should be relaxed when the heightened risk no longer exists.

The declaration of a higher security level should not be treated merely as an administrative announcement. Personnel must know which additional measures become applicable and who is responsible for implementing them. The transition between levels can itself create operational risks if instructions are delayed or contradictory. Port facilities and ships should therefore maintain readiness for rapid escalation. Equally, de-escalation is important because prolonged heightened restrictions can disrupt cargo operations, crew welfare and commercial activity. The graduated system works only when both escalation and restoration of normal operations are managed effectively.

10. COMPANY SECURITY OFFICER, SHIP SECURITY OFFICER AND PORT FACILITY SECURITY OFFICER

The ISPS Code establishes designated security officers to ensure that responsibility is not left undefined. The Company Security Officer functions at company level and coordinates security-related activities across the fleet. The Ship Security Officer implements the Ship Security Plan on board and acts as the operational link between the vessel and the company. The Port Facility Security Officer performs corresponding functions within the port facility and coordinates security measures with ships and authorities.

The effectiveness of these positions depends on authority, competence and resources. Designation alone is insufficient. Officers must understand the applicable legal requirements, have access to security information and be able to communicate with the persons who can make

operational decisions. They should also participate in drills, exercises and reviews so that weaknesses can be identified before an actual incident occurs.

Because these officers interact directly with seafarers and port workers, their decisions can influence working conditions. They should apply approved procedures consistently and avoid arbitrary restrictions. Professional conduct is particularly important in multinational maritime environments. Security officers should recognise that legitimate crew movement, emergency assistance and welfare needs form part of normal ship-port operations and should be addressed through the security plan rather than treated as exceptions without procedures.

The designation of security officers creates individual accountability, but it should not obscure institutional responsibility. A security officer cannot compensate for inadequate staffing, defective equipment or a poorly designed security plan. Companies and port authorities remain responsible for providing resources and establishing systems. The officers should also have access to senior management when a serious security concern arises. Their independence and professional competence are therefore important elements of the legal regime. Security functions should be treated as substantive management responsibilities rather than additional duties assigned without adequate time or authority.

11. RESPONSIBILITIES OF THE MASTER AND SHIPPING COMPANY

The Master has a special position under SOLAS Chapter XI-2 because security decisions may require immediate professional judgement. Regulation XI-2/8 confirms that the Master is not to be constrained by the company, charterer or any other person in exercising professional judgement over decisions necessary to maintain the security of the ship. This protection is important because commercial pressure should never override an urgent safety or security decision.

The shipping company has management responsibilities extending beyond the individual vessel. It must support security assessments, maintain the Ship Security Plan, designate appropriate security personnel, provide training and facilitate communication between ship and shore. A company that allocates security responsibilities without providing sufficient resources risks creating formal compliance without real protection.

The relationship between the Master and company should therefore be based on support rather

than interference. The Master must be able to respond to immediate threats, while the company should maintain systems that prevent predictable risks. Crew members also need a clear reporting mechanism for suspicious activities, security deficiencies and unsafe conditions. Such a culture encourages early reporting and reduces the possibility that minor weaknesses develop into major incidents.

The protection of the Master's professional judgement has particular labour significance. If a Master fears commercial retaliation for refusing to expose the vessel to an unreasonable security risk, the integrity of the system is compromised. Company policies should expressly support lawful security decisions and establish reporting mechanisms for disputes. The same principle applies to crew members who report suspicious conduct or security deficiencies. Effective maritime employment law should ensure that compliance with security duties is not converted into a source of unfair disciplinary pressure.

12. ACCESS CONTROL AND RESTRICTED AREAS

Access control is a fundamental security measure because unauthorised persons can compromise ships, cargo, equipment and personnel. A port facility should establish procedures for identifying persons seeking entry, determining whether access is authorised and limiting movement to areas appropriate to the person's function. Restricted areas should receive enhanced protection because they contain critical equipment, security systems or operational resources.

Access control must be risk-based and should distinguish between different categories of persons. Permanent port employees, contractors, ship crew, visitors and emergency personnel may require different levels of access. Procedures should be sufficiently secure to prevent impersonation and unauthorised entry but sufficiently efficient to avoid unnecessary disruption. Records of access may also support investigations after an incident.

For seafarers, access control is closely connected with the practical realities of shipboard employment. Crew members may need to move between ship and port, obtain medical treatment or communicate with agents. Clear procedures for legitimate movement can reduce conflict between security personnel and workers. Security should be achieved through reliable authorisation and monitoring rather than through arbitrary barriers that disregard established employment needs.

Access-control systems should also provide procedures for persons whose presence is necessary but temporary. Ship repair teams, surveyors, pilots, agents, medical personnel and emergency responders may need access at short notice. A rigid system that cannot accommodate legitimate operational needs may encourage personnel to bypass controls. The better approach is preauthorised categories, temporary passes, escorts where appropriate and clear emergency exceptions. Records should be maintained so that exceptional access remains accountable. Such arrangements protect both security and efficient port operations.

13. SHIP SECURITY ALERT SYSTEM AND SECURITY

COMMUNICATION

The Ship Security Alert System is designed to raise an alert when the security of the ship is threatened or has been compromised. Its significance lies in the ability to communicate a security concern without necessarily requiring the crew to confront the threat directly. Security alerts can initiate assistance from competent authorities and support coordinated response. The system therefore forms an important connection between shipboard security and governmental security mechanisms.

Security communication must be reliable, confidential where necessary and understood by all relevant personnel. Ships may communicate with port facilities, company security officers, maritime administrations and emergency services. Procedures should identify who may activate an alert, what information should be transmitted and what actions follow. False alarms should be managed carefully, but fear of criticism should not discourage genuine reporting.

Training is essential because a communication system is only as effective as the people who know how to use it. Drills should test not only equipment but also the decision-making chain. Crew members should know how to recognise a security emergency, whom to inform and how to protect themselves and others while assistance is mobilised.

Security communication should be tested for reliability in adverse conditions. Ships may experience equipment failure, poor connectivity, language barriers or confusion during emergencies. Backup communication methods are therefore important. The legal framework should also protect the confidentiality of sensitive security information while ensuring that the relevant authorities receive enough information to respond. A reporting culture is strengthened

when crew members know that good-faith security reports will be taken seriously. False reporting should be addressed, but excessive punishment for honest mistakes may discourage early warning.

14. DECLARATION OF SECURITY

A Declaration of Security is an important mechanism for establishing agreement on security responsibilities between a ship and a port facility or another ship where appropriate. It is particularly useful when security requirements differ from ordinary arrangements or when specific circumstances create additional risks. The declaration helps clarify which party will undertake particular measures and provides a documented basis for coordination.

The value of a declaration lies in reducing uncertainty at the ship-port interface. Without clear allocation of responsibility, a security measure may be assumed to be the responsibility of another party. This can create gaps precisely where cargo, personnel or equipment are transferred. The declaration should therefore be prepared when the circumstances warrant it and should reflect the actual security conditions rather than becoming a routine form with no operational significance.

The declaration can also support accountability after an incident. Records showing who agreed to undertake particular security measures may assist investigation and corrective action. However, documentation should not substitute for active security. The ultimate purpose is operational coordination, and the parties should ensure that the agreed measures are understood and implemented by the personnel who are responsible for carrying them out.

The declaration mechanism is particularly valuable where the security responsibilities of the ship and port facility are not identical. It can identify the measures that each party will undertake and can establish a common understanding before operations begin. This is important during unusual cargo operations, high-risk visits or heightened security conditions. The declaration should be reviewed when circumstances change. Its legal value is greatest when it reflects real operational responsibility rather than simply reproducing standard language without consideration of the particular ship-port interface.

15. SECURITY DRILLS, EXERCISES, AUDITS AND VERIFICATION

A security plan cannot be considered effective merely because it has been approved. Drills and

exercises are necessary to determine whether personnel understand their duties and whether communication systems work under pressure. Exercises can reveal practical weaknesses such as unclear command structures, inadequate access arrangements, equipment failures or delays in communication. Corrective action following exercises is therefore a core element of continuous security improvement.

Audits provide a more systematic form of verification. They can examine whether security assessments remain current, whether plans are implemented, whether security officers are performing their functions and whether records and procedures are maintained. Verification should not become a purely documentary process. Inspectors and auditors should consider actual practice and the ability of personnel to respond to realistic scenarios.

For marine employment, drills and audits should take account of crew composition, working hours and fatigue. Training should be delivered in a manner that is understandable to multinational crews and should not place seafarers at unnecessary risk. A security culture is strongest when personnel understand why procedures exist and are encouraged to report weaknesses. Continuous improvement is therefore both a management and labour issue.

The distinction between an exercise and an audit should be preserved. An exercise tests whether people and systems can respond to a simulated event, while an audit examines whether the management system conforms to applicable requirements and remains effective. Both are necessary. Lessons from exercises should feed into corrective action, and audit findings should be followed to closure. The process should not become punitive to the extent that personnel hide mistakes. A learning-oriented approach can identify systemic causes and improve future performance.

16. FLAG STATE RESPONSIBILITIES

The flag State is the primary regulatory State for a ship flying its flag. Under international maritime law, it is expected to exercise effective jurisdiction and control over administrative, technical and social matters on board. In the security field, the flag State establishes the national system for implementing SOLAS Chapter XI-2 and the ISPS Code, including designation of competent authorities, approval and verification arrangements and communication with other States.

Under the MLC, 2006, the flag State also bears primary responsibility for ensuring that ships flying its flag comply with maritime labour standards. This includes inspection and certification systems, enforcement of working and living conditions and access to complaint mechanisms. The combination of security and labour responsibilities demonstrates that the flag State must consider the vessel as both a security unit and a workplace.

An effective flag State therefore needs adequate inspectors, recognised organisations where applicable, reporting systems and enforcement powers. Weak flag State administration may transfer excessive burdens to port States and create inconsistent protection. International cooperation and information exchange can improve compliance, but they do not remove the fundamental responsibility of the flag State to exercise effective jurisdiction over ships entitled to fly its flag.

The effectiveness of flag State control is influenced by the quality of its maritime administration. A State with adequate legislation but insufficient inspectors may fail to provide effective control. Flag States should maintain registers, certification systems, inspection programmes and mechanisms for receiving complaints and security information. They should also cooperate with port States when deficiencies are detected. For seafarers, effective flag State administration provides a first layer of protection because the ship is the primary workplace and many employment issues arise while the vessel is at sea.

17. PORT STATE RESPONSIBILITIES AND PORT STATE CONTROL

Port State control is an important enforcement mechanism because foreign ships enter ports outside the jurisdiction of their flag States. A port State can inspect ships in accordance with applicable international law and treaty obligations and can require corrective action where serious deficiencies are identified. This complements rather than replaces flag State control.

Under the MLC, 2006, port State responsibilities provide an additional layer of protection for seafarers. Port State control officers may examine documents and, where warranted, conduct more detailed inspections of working and living conditions. Serious deficiencies affecting seafarers may justify corrective measures and, in appropriate circumstances, detention. The ILO has developed detailed guidelines to assist inspectors in carrying out these responsibilities consistently.

In the security context, port authorities and competent security agencies may verify whether ships have appropriate security arrangements and may take measures where security concerns arise. The challenge is to enforce standards without causing unnecessary delay. Port State control should therefore be risk-based and professional, with findings recorded clearly and communicated to the ship and, where necessary, the flag State.

Port State control is sometimes described as a secondary mechanism, but in practice it can be decisive where flag State enforcement is weak. Its legitimacy depends on consistent application of international standards and avoidance of discriminatory treatment. Inspectors should distinguish serious deficiencies from minor administrative irregularities and should communicate findings clearly. Cooperation with regional port State control regimes can promote consistency. From the labour perspective, port State inspection can provide seafarers with an external avenue for raising serious problems that have not been resolved on board.

18. LABOUR-SUPPLYING STATE RESPONSIBILITIES

The MLC, 2006 recognises that the State in which seafarers are recruited can have an important role in protecting workers even though the ship may fly a foreign flag. Regulation 5.3 requires labour-supplying States to establish effective inspection and monitoring systems for their responsibilities. This creates an important legal connection between national labour administration and the international maritime employment relationship.

Labour-supplying State responsibilities are particularly significant in countries that provide large numbers of seafarers to the global fleet. Recruitment and placement agencies must be regulated, monitored and subject to appropriate enforcement. Seafarers should have access to information and complaint mechanisms, and unlawful practices should be addressed through effective sanctions. Proper recruitment also assists shipowners and States in ensuring that employment relationships are genuine and documented.

Cooperation among labour-supplying, flag and port States is essential. A seafarer may experience a recruitment problem in one jurisdiction and a working-condition problem in another. Fragmented enforcement can leave gaps. The MLC addresses this through a network of responsibilities, demonstrating that protection of maritime workers requires coordination across the entire employment chain.

Labour-supplying States occupy a distinctive position because they regulate services that connect workers with international employers. Their responsibility should not be reduced to issuing licences to recruitment agencies. Effective regulation requires inspections, complaint handling, records and cooperation with foreign authorities. Where a recruitment agency fails, the consequences may include debt, abandonment or forced continuation of an employment relationship. Strong labour-supplying State oversight therefore contributes to the prevention of exploitation before the seafarer reaches the vessel and reduces the likelihood of disputes during employment.

19. RECRUITMENT AND PLACEMENT OF SEAFARERS

Recruitment and placement are important because exploitation can occur before a seafarer joins a ship. International labour standards seek to ensure that recruitment services operate responsibly and that seafarers are not subjected to abusive practices. Regulation 1.4 and Standard A1.4 of the MLC provide the principal international framework for recruitment and placement services in States where such services operate.

A sound recruitment system should include licensing or authorisation, record keeping, inspection and complaint procedures. Agencies should provide accurate information about employment conditions and should not use fraudulent representations. Effective supervision also helps prevent unlawful fees and deceptive contracts. Digital recruitment has increased the need for oversight because seafarers may now be recruited through online platforms that operate across borders.

Recruitment regulation also supports maritime security. Shipowners need confidence that the persons joining ships are genuine workers with appropriate qualifications and documentation. Security should not, however, be used to justify unnecessary or discriminatory recruitment barriers. The objective should be lawful verification combined with fair access to employment. Labour administration and security administration should exchange information through lawful and proportionate mechanisms.

Recruitment regulation also has a direct relationship with fair competition in shipping. If some operators obtain labour through agencies that charge unlawful fees or provide misleading information, compliant operators may face competitive disadvantages. The MLC's approach seeks to establish minimum standards across the industry. National authorities should therefore

treat recruitment regulation as part of maritime governance rather than ordinary employment administration. Complaint procedures should be accessible even when the worker is already at sea, and agencies should retain records that allow authorities to investigate cross-border recruitment practices.

20. MLC, 2006 AND THE PROTECTION OF SEAFARERS

The Maritime Labour Convention, 2006 is often described as a comprehensive maritime labour instrument because it consolidates minimum standards for seafarers' employment and living conditions. It covers minimum requirements for work, conditions of employment, accommodation, food, health protection, medical care, welfare and social security. Its enforcement architecture is particularly relevant to this analysis because it assigns responsibilities to flag States, port States and labour-supplying States.

The Convention uses a combination of mandatory rights and implementation mechanisms. Flag States must establish inspection and certification systems; port States may inspect foreign ships; and labour-supplying States must regulate recruitment and placement services within the scope of their responsibilities. The system is designed to prevent unfair competition by ensuring that minimum labour standards are applied across the maritime industry.

Security and labour protection should be understood as mutually reinforcing. Seafarers who are adequately rested, trained, medically supported and treated fairly are better positioned to respond to security threats. Conversely, a security environment that unnecessarily restricts access to medical treatment, welfare services or lawful movement can undermine the purpose of maritime labour standards. Effective maritime governance must therefore coordinate both areas.

The MLC's enforcement model is significant because it recognises that maritime employment is inherently international. A seafarer cannot always rely on the law of the State of nationality or recruitment. The Convention therefore distributes duties among the flag State, port State and labour-supplying State. The system is intended to create overlapping protection rather than complete duplication. Effective enforcement requires these jurisdictions to communicate and to respect the different functions assigned to each. This approach is especially valuable where an employment dispute crosses several legal systems.

21. MARITIME SAFETY, SECURITY AND SEAFARER WELFARE

The distinction between safety, security and welfare is useful for legal classification, but the practical reality on board is integrated. A security incident may lead to fire, collision, injury or pollution. A fatigued crew may be less capable of responding effectively to an unlawful intrusion. A lack of medical support can make the consequences of an incident more severe. The legal regime should therefore recognise the operational interdependence of these areas.

The MLC addresses working and living conditions, while SOLAS and the ISPS Code address safety and security. These instruments operate through different institutional mechanisms but ultimately protect human life at sea. Companies should coordinate their safety management and security management procedures and ensure that crew members receive compatible instructions. Port authorities should similarly coordinate emergency, safety and security agencies.

Welfare should not be treated as an optional benefit that disappears during security planning. Shore access, medical assistance, communication with family and timely repatriation can be essential to seafarers' wellbeing. Where security circumstances require restrictions, authorities should use the least restrictive measures consistent with the threat and restore ordinary welfare arrangements as soon as reasonably possible.

A rights-sensitive security regime should recognise that welfare failures can become operational risks. Excessive working hours, inadequate rest or prolonged inability to obtain medical assistance can impair judgement. Security planning should therefore consider crew fatigue and realistic staffing levels. Welfare measures also support morale and cooperation with security procedures. Seafarers are more likely to report suspicious conduct and follow emergency instructions when they have confidence that management and authorities will treat them fairly. Security is consequently strengthened by decent employment conditions.

23. ISM CODE AND THE INTEGRATION OF SAFETY AND SECURITY

MANAGEMENT

The ISM Code and ISPS Code address different risks but share a management-system philosophy. The ISM Code promotes safe management and operation of ships and pollution prevention, while the ISPS Code focuses on security against unlawful interference. Both

require defined responsibilities, procedures, communication, training, reporting and review. Companies can therefore coordinate the systems while maintaining compliance with the separate legal requirements.

Integration is particularly valuable during emergencies. A security incident can rapidly become a safety event, and the crew may need to respond to both dimensions simultaneously. Procedures should therefore avoid contradictory instructions. The company's safety management system and security management arrangements should identify how information is shared, how command decisions are made and how external assistance is requested.

Integrated management can also improve labour protection. Security and safety failures may increase workload, fatigue and stress among crew members. A system that identifies these risks and plans realistic responses supports decent working conditions. Continuous improvement should be based on incident reports, drills, audits, complaints and lessons learned from other vessels.

The strongest management systems connect incident reporting, corrective action and review across safety and security functions. A near miss involving unauthorised access, for example, may reveal a weakness in both security procedures and safety management. Companies should avoid separate reporting cultures in which information remains within departmental boundaries. Senior management should review trends and allocate resources accordingly. Integration also helps ensure that security measures do not unintentionally create new safety hazards, such as blocked emergency routes or excessive delays in access to medical services.

22. STCW AND SECURITY TRAINING

The STCW Convention establishes international standards for seafarer competence and training. Security competence is important because many crew members participate in ship security measures even when they are not designated security officers. Training can cover security awareness, recognition of threats, emergency procedures, access control and appropriate response. The level of training should correspond to the duties assigned to the seafarer.

Security training should be practical and regularly reinforced. Classroom knowledge alone may not prepare a crew for a rapidly developing incident. Drills and exercises allow personnel to

practise communication, muster arrangements, access restrictions and reporting. Training should also consider the multicultural composition of modern crews and use procedures that are clear to persons with different language backgrounds.

Employers should ensure that security training does not become a paper-compliance exercise. Certificates are important evidence of competence, but the real objective is safe performance. Training should be reviewed when security plans change, when new equipment is introduced or when exercises identify weaknesses. Proper training protects both the ship and the employment rights of seafarers by reducing avoidable risk.

Training should be periodically updated because security threats and technology change. A certificate obtained years earlier does not guarantee that a seafarer understands a newly introduced access system or cyber threat. Refresher training and onboard familiarisation are therefore important. Companies should also evaluate whether training is understood rather than merely completed. Language and literacy considerations should be addressed through clear instructions and demonstrations. Training is a preventive legal measure because it reduces the probability that human error will defeat otherwise adequate security controls.

24. UNCLOS AND THE INTERNATIONAL LEGAL FRAMEWORK

UNCLOS provides the broader legal framework within which maritime activities take place. It establishes rules concerning maritime zones, navigation, jurisdiction and responsibilities of States. Specialised conventions such as SOLAS and the ISPS Code operate within this broader international legal order. The existence of a specialised security instrument does not eliminate the importance of general rules concerning jurisdiction and cooperation.

The division of jurisdiction is especially relevant when a security incident involves several States. The flag State has jurisdiction over its ship in many circumstances, while a port State exercises authority within its ports and internal waters subject to international law. Coastal and other States may have relevant powers depending on the location and nature of the incident. Clear coordination is therefore necessary to avoid jurisdictional uncertainty during emergencies.

UNCLOS also demonstrates that maritime governance is based on a combination of national jurisdiction and international cooperation. Security threats do not stop at maritime boundaries.

Effective enforcement therefore requires information exchange, mutual assistance and respect for applicable international obligations. The ISPS Code adds a specialised operational framework to this wider legal structure.

The interaction between UNCLOS and specialised conventions shows that jurisdiction must be analysed according to the location, vessel, persons involved and applicable treaty obligations. Maritime security incidents can involve criminal law, immigration, customs, labour and maritime safety simultaneously. No single instrument answers every question. Authorities should therefore identify the applicable legal basis before exercising powers and should cooperate where several jurisdictions are involved. Respect for international law is important not only for legality but also for predictable treatment of ships and seafarers moving between States.

25. INDIAN LEGAL FRAMEWORK: MERCHANT SHIPPING ACT, 2025

India's Merchant Shipping Act, 2025 is a significant development in the domestic maritime legal framework. It consolidates and amends the law relating to merchant shipping and expressly seeks to ensure compliance with India's obligations under maritime treaties and international instruments. The Act came into force on 15 March 2026. It includes a dedicated regulatory structure addressing safety and security as well as maritime labour and related enforcement.

The Act provides for a body concerned with the security of vessels and port facilities and establishes provisions dealing with safety and security requirements. It also contains enforcement and control mechanisms. These provisions provide a domestic statutory foundation through which India can give effect to international maritime obligations. The Act should, however, be read with subordinate legislation, rules, notifications and applicable IMO instruments because the ISPS regime is technically detailed.

For marine employment, the Act is relevant because security is implemented within a broader framework governing seafarers, safe manning, training, ship operations and welfare. Effective administration requires coordination between the Director-General of Maritime Administration, port authorities and other government agencies. The modern Indian framework therefore moves towards an integrated conception of maritime governance rather than treating security as an isolated port function.

The 2025 Act represents an important modernisation of India's merchant shipping law. Its relevance to this analysis lies in its explicit treatment of security alongside safety and maritime labour. The Act should be understood as part of a broader implementation structure rather than as a replacement for technical international standards. Regulations, rules and administrative directions will remain important because security requirements depend on operational detail. Indian authorities should therefore maintain alignment between domestic requirements and IMO standards so that Indian ships and ports remain compatible with international shipping practices.

26. INDIAN PORTS ACT, 2025 AND PORT SECURITY GOVERNANCE

The Indian Ports Act, 2025 consolidates the law relating to ports and provides a framework for integrated port development, navigation, safety, security, emergencies and related matters. Its importance to the present analysis lies in the fact that port security is not governed solely by the ISPS Code. International obligations require domestic institutional arrangements, and the national port statute provides an important layer of that domestic framework.

Port security governance requires coordination between port authorities and national maritime security institutions. The port may operate through public authorities and private terminal operators, while customs, immigration, police and other agencies exercise their own legal functions. A coherent statutory framework can help define responsibilities, powers and coordination mechanisms. The effectiveness of the system ultimately depends on implementation at the individual port facility.

The Indian Ports Act should therefore be read together with the Merchant Shipping Act, 2025 and the international security regime. Where port operations affect seafarers, security arrangements should also be consistent with applicable labour standards. The objective should be an integrated port in which security, navigation, occupational safety, environmental protection and worker welfare are planned together.

Port governance under the 2025 Act must operate alongside the specialised ISPS regime. The existence of general port powers does not remove the need for an approved security system at facilities covered by SOLAS Chapter XI-2. Coordination is particularly important where public and private port operators share functions. Security requirements should be incorporated into operational authorisations, contracts and emergency arrangements. A port's legal framework

should also preserve continuity of essential services during security incidents, because disruption of medical, safety or emergency functions may directly affect seafarers.

27. ROLE OF THE DIRECTORATE GENERAL OF SHIPPING AND PORT AUTHORITIES

India's maritime administration performs a central role in implementing international maritime standards. The Directorate General of Shipping and the wider maritime administration are responsible for regulatory, inspection, certification, seafarer and safety functions. In the security context, competent authorities must ensure that ships and port facilities operate within the ISPS framework and that relevant information is communicated to the appropriate agencies.

Port authorities and terminal operators have practical responsibility for implementing security procedures at the facility level. Their functions include access management, surveillance, coordination with ships and response to incidents. Because many port functions are carried out by private entities and contractors, security governance must extend beyond the formal port authority. Contracts and operating procedures should require compliance with approved security arrangements.

Effective governance also requires coordination with immigration, customs, police, coastal security and emergency services. Fragmented responsibilities can create gaps or duplicate controls. India can strengthen the system through integrated command arrangements, common training, regular exercises and secure information sharing. Seafarers benefit when these arrangements produce predictable procedures rather than repeated and inconsistent checks.

The effectiveness of India's maritime security framework ultimately depends on institutional coordination. The maritime administration, port authorities, security agencies, customs, immigration and law-enforcement bodies may possess different statutory powers and information. Joint exercises and common operating procedures can reduce gaps. Port authorities should also maintain effective communication with ship agents and security officers. For seafarers, predictable administrative procedures are important because inconsistent requirements can cause delays in joining, disembarking or accessing welfare services. Efficient administration is therefore part of both security and labour protection.

28. COMPLIANCE, INSPECTION AND ENFORCEMENT

The credibility of maritime security law depends on effective enforcement. Compliance may be examined through certification, verification, audits, inspections, drills and exercises. A security plan or certificate demonstrates formal compliance, but inspectors must also consider whether the prescribed measures are actually implemented. The distinction between paper compliance and operational compliance is particularly important in risk-based regulation.

Port State control is an important supplementary mechanism because foreign ships may operate under flags whose administrative systems are difficult for a port State to observe directly. International inspection procedures seek to identify serious deficiencies while avoiding unnecessary delay. Under the MLC, inspectors also consider seafarers' working and living conditions. Where serious deficiencies threaten safety, security or welfare, corrective measures may be required and detention may be justified under applicable law.

Enforcement should be proportionate and transparent. Minor procedural deficiencies may be corrected without severe sanctions, while serious security failures may require immediate intervention. Authorities should record findings, communicate corrective requirements and follow up to confirm compliance. Effective enforcement is not measured simply by the number of penalties but by the extent to which inspections prevent harm and improve future performance.

Enforcement should also incorporate procedural fairness. Shipowners and Masters should receive clear information about deficiencies, the legal basis for corrective measures and the steps required for release where a vessel is detained. At the same time, serious risks should not be overlooked merely because compliance would be commercially inconvenient. A balanced system protects both maritime safety and the rights of regulated parties. Records of inspections and corrective action can support accountability and help authorities identify recurring problems across ships or port facilities.

29. CONTEMPORARY CHALLENGES, CRITICAL ANALYSIS AND RECOMMENDATIONS

One of the greatest challenges is the changing nature of maritime security threats. Ports and ships increasingly depend on digital systems, automated cargo handling and networked

communications. Cyber incidents can therefore disrupt port operations without a conventional physical intrusion. Security frameworks must evolve so that cyber risk is included in assessments and management systems. At the same time, traditional risks such as unlawful entry, smuggling, sabotage and terrorism remain relevant.

A second challenge is fragmentation of authority. Modern shipping connects multiple States and private actors, while security and labour responsibilities are divided among different institutions. The legal allocation of responsibility is necessary, but poor coordination can produce gaps. India can strengthen implementation by improving inter-agency communication, integrating safety and security exercises, maintaining effective recruitment oversight and ensuring that port and flag State inspectors receive specialised training.

A third challenge is maintaining proportionality. Security measures that are unnecessarily restrictive can disrupt maritime trade and interfere with seafarer welfare, while weak measures can expose ships and ports to serious danger. The recommended approach is risk-based and rightsensitive: reliable threat assessments, clear security plans, trained personnel, effective complaint systems, regular audits, strong cybersecurity, protection of confidential information and continuous review. Security should protect legitimate maritime activity rather than obstruct it.

The future of maritime security should therefore be based on integrated governance. Port authorities, maritime administrations, employers, security agencies and labour institutions should share responsibility within clearly defined legal boundaries. Seafarers should be treated as trained participants in security systems, not simply as objects of control. Their welfare, rest, medical needs and lawful movement should be incorporated into emergency and security planning. This approach is more likely to produce a resilient maritime transport system.

Future regulation should increasingly address cyber-physical risks, supply-chain disruption and the use of automated port systems. The legal framework should remain technology-neutral enough to accommodate innovation while requiring operators to manage identifiable risks. India should also strengthen coordination between maritime labour inspection and port security administration. A further recommendation is the development of standard procedures for emergency welfare access during heightened security levels. Such procedures would reduce uncertainty and ensure that security measures do not unintentionally prevent essential medical care or lawful repatriation.

30. CONCLUSION

The ISPS Code has transformed international maritime security by creating a mandatory, riskbased framework for ships and port facilities through SOLAS Chapter XI-2. Its importance extends beyond physical protection because it establishes responsibilities, procedures, security levels, assessments, plans, officers and verification mechanisms. The Code demonstrates that maritime security is a continuing management function rather than a response reserved for extraordinary incidents.

The relationship between security and marine employment is equally significant. Flag States, port States and labour-supplying States each have distinct responsibilities under international law. The MLC, 2006 provides a complementary labour framework through inspection, certification, port State control and regulation of recruitment and placement. Seafarers are central to both systems because their competence, welfare and working conditions affect the resilience of ships and ports.

India's Merchant Shipping Act, 2025 and Indian Ports Act, 2025 provide an important contemporary domestic framework for implementing maritime safety and security. Their effectiveness will depend on administrative coordination, appropriate subordinate rules, inspection capacity and cooperation with international institutions. The ultimate objective should be a maritime system in which security measures are effective, proportionate and compatible with decent conditions of work. Protecting ships and ports and protecting seafarers are not separate goals; they are essential elements of responsible maritime governance.

Ultimately, the legitimacy of maritime security law depends on whether it protects human life while enabling lawful maritime commerce. The ISPS Code provides the security architecture, the MLC supplies the labour-protection framework, and Indian legislation provides domestic institutional mechanisms. Their combined effectiveness depends on competent administration, adequate resources and cooperation among States and industry. A modern maritime security regime should therefore be measured by resilience: the ability to prevent incidents, respond effectively when they occur and preserve the safety, dignity and lawful interests of seafarers throughout the process.

REFERENCES

1. International Maritime Organization, International Convention for the Safety of Life at Sea, 1974, as amended.
2. International Maritime Organization, International Ship and Port Facility Security (ISPS) Code, Part A and Part B.
3. International Maritime Organization, SOLAS Chapter XI-2: Special Measures to Enhance Maritime Security.
4. International Maritime Organization, Maritime Security: Official IMO materials on ship and port facility security.
5. International Maritime Organization, International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978, as amended.
6. International Maritime Organization, International Safety Management Code, as amended.
7. International Maritime Organization, Port State Control: Procedures for Port State Control, 2025, IMO Resolution A.1206(34).
8. International Labour Organization, Maritime Labour Convention, 2006, as amended.
9. International Labour Organization, Guidelines for Flag State Inspections under the Maritime Labour Convention, 2006, as amended.
10. International Labour Organization, Guidelines for Port State Control Officers Carrying Out Inspections under the Maritime Labour Convention, 2006, as amended.
11. International Labour Organization, MLC, 2006: What it is and what it does.
12. United Nations, United Nations Convention on the Law of the Sea, 1982.
13. Government of India, The Merchant Shipping Act, 2025, Act No. 24 of 2025.
14. Government of India, The Indian Ports Act, 2025.
15. Directorate General of Shipping, Government of India, Port Security/ISPS Code, official regulatory materials.

Official online materials consulted include the IMO and ILO websites and India Code. Accessed 04 September 2026.

16. International Maritime Organization, International Ship and Port Facility Security (ISPS) Code, consolidated edition and subsequent amendments.
17. International Maritime Organization, 'SOLAS XI-2 and the ISPS Code', official maritime security materials.
18. International Maritime Organization, 'Maritime Security', official IMO materials.
19. International Labour Organization, Maritime Labour Convention, 2006, as amended, including the 2022 amendments.
20. International Labour Organization, Regulation 5.3 and Standard A5.3 of the Maritime Labour Convention, 2006, concerning labour-supplying responsibilities.
21. International Labour Organization, Guidelines for Flag State Inspection under the Maritime Labour Convention, 2006, as amended.
22. International Labour Organization, Guidelines for Port State Control Officers Carrying Out Inspections under the Maritime Labour Convention, 2006, as amended.
23. International Maritime Organization, International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978, as amended.
24. International Maritime Organization, International Safety Management Code, as amended.
25. United Nations, United Nations Convention on the Law of the Sea, 1982.
26. Government of India, The Merchant Shipping Act, 2025, Act No. 24 of 2025.
27. Government of India, The Indian Ports Act, 2025, Act No. 27 of 2025.
28. Government of India, Directorate General of Shipping, Port Security / ISPS Code, official regulatory materials.
29. Government of India, India Code, official text and enforcement information concerning the Merchant Shipping Act, 2025.
30. Government of India, India Code, official text and enforcement information concerning the Indian Ports Act, 2025.