



The International Ship and Port Facility Security Code (ISPS): Possible Areas to Update

Due to the changing nature of new threats to port protection and security, it is necessary to adapt the ISPS code to these new environments to guarantee the integrity of port and maritime operations. In this context the ISPS code requires the strengthening of measures to address current threats. Therefore, updating the ISPS code to consider and incorporate threats not included in it should be a priority. This would help to minimize risks, improve ISPS code procedures and have better responses to threats with the uniform criteria and under regulated standards or norms.

The Code for the Protection of Ships and Port Facilities, known by its acronym, ISPS, was adopted by the International Maritime Organization (IMO), because of the attacks of September 11, 2001. During the meeting of the 22nd Assembly of the IMO, held in November 2001, it was agreed to develop new legislative measures relating to the security of ships and port facilities, which were approved by resolutions adopted on December 12, 2002 at the Diplomatic Conference on Maritime Security of the Contracting Governments of the International Convention for the Safety of Life at Sea (SOLAS Convention).

The ISPS Code raises aspects related to port protection and security, encompassing certain norms and standards for port protection and security. Since its implementation on 1 July 2004, the ISPS Code has formed the basis of mandatory security standards for international maritime transport, designed to address a wide range of threats to the safety and security of ships and vessels. port facilities.

The ISPS code seeks to minimize the risks of illegal activities that could cause a tragic impact on maritime transport and port infrastructure, including elements such as:

- a) The physical protection of ships,
- b) The implementation of preventive measures in port facilities,
- c) Training of personnel and
- d) International cooperation to address possible threats.

The ISPS code is composed of mandatory measures and guidelines for the protection of ships and port facilities and applies only to ships that carry out international routes with a minimum tonnage of 500 Gross Register Tons (GRT), for mobile submarine drilling units on the high seas, and for port facilities that provide service to said vessels and mobile units. ([Chapter XI -2 of the SOLAS Convention and the ISPS Code](#))



The objectives of the ISPS Code are:

- a) Establish an environment that guides international cooperation in the maritime field, to identify threats to port protection and security, and to take preventive measures against these and acts of terrorism.
- b) Define the corresponding functions and responsibilities of the contracting governments and parties at the national and international level to guarantee maritime security.
- c) Guarantee the rapid and effective collection and exchange of information related to maritime security.
- d) Provide methods to carry out protection evaluations to have plans and procedures that allow changes in protection levels to be implemented.
- e) Guarantee the certainty of having adequate maritime protection measures.

The ISPS Code constitutes a set of rules to generally improve port protection and security in the field of international maritime trade, providing contracting governments with justified guidance for the implementation of security plans. port protection and security.

However, the permanent evolution of risks and challenges raises new concerns that require a proactive and adaptive response, requiring continuous review and updating of the ISPS code and the implementation of updated measures to maintain safety and security in port and maritime environments. This imminent and necessary update is needed to provide guidance to OPIPs and port authorities on how to solve these new threats.

For example:

- a) The current use of aerial and underwater drones is a big threat to port protection and security that is important to consider in a timely manner, since with these drones terrorist attacks can be carried out on port facilities and ships. This leads to the need to have established regulations for their use. Importantly, port facilities and ships must have anti-drone systems to maintain port protection and security.
- b) Smuggling, both of drugs and people, is increasingly complex and is carried out through organized crime, which is why they use schemes to evade detection and carry out smuggling, such as divers transporting submerged drugs in the vicinity of port facilities and ships.
- c) Maritime piracy is a global problem and is catalyzed due to the few economic opportunities of the populations, likewise the lack of protection and security in the geographical locations of some routes provide opportunities for piracy, piracy attacks cause significant economic losses putting the goods on the ships' commercial routes at risk.



OAS | More rights
for more people



CIP | Inter-American
Committee on Ports



- d) Cyber-attacks are threats to everything digital, increasing their potential with the growing digitalization of port and maritime systems. The risks of cyber-attacks and hacking have become more common and critical to port facilities and ships, which jeopardizes the safety and security as well as the operability of these environments. This can include unauthorized access to maritime traffic control systems, manipulation of cargo data or even the possibility of causing very serious incidents. Likewise, technological developments have expanded access to resources to terrorist groups, increasing their financing, recruitment, training and propaganda capacity.
- e) Geopolitical tensions and international conflicts may pose a threat to compliance with the ISPS Code. Ports and strategic shipping routes may be subject to disputes and conflicts, posing additional challenges for the protection and security of port facilities and ships. The possibility of confrontations or incidents related to these conflicts requires special preparation to guarantee the safe continuity of port operations in high-tension environments.
- f) Climate change and natural disasters pose an increasing threat to the safety and security of port facilities and ships; extreme weather events such as hurricanes, storms and tsunamis can cause significant damage to port infrastructure and put at risk jeopardize the safe navigation of ships.
- g) The sophistication of terrorist tactics, as well as the possibility of coordinated attacks from multiple locations, poses a serious risk that requires constant review and update of the port protection and security measures prescribed in the ISPS code, which must be adequate to today's new threats.



These threats can be identified as elements that have not been considered in the implementation of the ISPS Code, which may cause its compliance to be inefficient in the face of acts caused by current threats. Acts of terrorism, whether with the use of explosives using aerial or underwater drones or the infiltration of malicious individuals with explosive devices, represent a constant challenge to port protection and security.

Considering that several of the current threats are not contemplated in the ISPS code and that they are increasingly pose a greater risk to port protection and security, it is imperative that the Port Authorities of the Contracting Governments of the SOLAS Convention express and propose to the Committee of Maritime Safety of the International Maritime Organization (IMO), the adoption of new measures and amendments to update the ISPS Code, in order to increase port protection and security in the face of current threats that are not considered in the ISPS code.

The update of the ISPS Code will help provide Port Authorities of SOLAS Contracting Governments with a harmonization of standards and best practices for the development and implementation of port security and protection plans to reduce the risks to current threats by adapting accordingly the situation of each port.

For its part, the Inter-American Committee on Ports (CIP) seeks to advise and support the entire port community, which is why on its web portal: <https://portalcip.org/tags/port-protection-and-security-tag/documents/?lang=en> various documents and resources are available on port protection and security issues, which are of great value and interest to be consulted and thus expand information in the face of the challenges of new threats to port protection and security.