INTERNATIONAL SHIP AND PORT FACILITY SECURITY (ISPS) CODE — WHAT DOES IT MEAN FOR FISHING VESSEL SECURITY?

John P. Hogan[1] and Lindsay Chapman[2]
Secretariat of the Pacific Community

Introduction

The International Maritime Organization (IMO) has introduced a range of security measures under the Safety of Life at Sea (SOLAS) Convention, through amendments that establish an international framework by which ships and port facilities can detect and deter acts that threaten maritime transport security. SOLAS regulations include the International Ship and Port Facility Security (ISPS) Code. This code applies to all cargo ships 500 gross tons and larger, all passenger ships on international voyages, and to the port facilities serving such ships. It does not apply to fishing vessels or to merchant vessels less than 500 gross tons.

The ISPS Code has been in force since 1 July 2004 for those states that are parties to SOLAS. While the ISPS Code is designed to deal with maritime security, it is not about responding to terrorist incidents. Rather, it is a comprehensive preventive regime that takes a risk management approach to protecting ships and port facilities.

All Pacific Island countries and territories (PICTs) are currently in compliance with the Code. They face a challenge, however, in effectively implementing the Code on an ongoing basis, in relation to both port facilities and ships using such ports. One of the concerns raised at the 2004 meeting of the Pacific Islands Forum Regional Security Committee was the fact that the Code's security measures do not apply to fishing vessels. The main concerns relating to fishing vessels include piracy, the smuggling of people and/or illegal goods (drugs, firearms, alcohol, etc.) and stowaways. PICTs are to ascertain ways to apply either the Code or alternatively some other security arrangement that will be agreeable to their fishing industry, as well as other fishing vessel Flag States.

The ISPS Code in a nutshell

The ISPS Code provides a standardised and consistent international framework for identifying and evaluating security risks to ships and port facilities used in international trade, and a means of taking appropriate preventive measures against such risks. The Code is specifically designed to cover security in regard to terrorism or a terrorist threat, and reflects a strong risk management approach. Its fundamental principle is that each ship or port facility faces different types of risks, and these risks must be well understood and an assessment made so that appropriate security measures can be put in place to protect life, property, and the environment.

The ISPS Code is divided into two parts: those that are mandatory and those that are recommended. States that are party to SOLAS decide the extent to which the Code should be applied to those port facilities within their territory that are used primarily by ships engaged on domestic voyages, but which may occasionally serve ships arriving or departing on an international voyage. The Code does not apply to warships, naval auxiliaries or other ships owned or operated by Contracting Governments and used only on non-commercial service. More importantly, the Code does not apply to fishing vessels.

The functional requirements of the Code include gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments; requiring the maintenance of communication protocols for ships and port facilities; preventing unauthorised access to ships, port facilities and their restricted areas; preventing the introduction of unauthorised weapons, incendiary devices or explosives to ships or port facilities; providing means for raising alarms in reaction to security threats or security incidents; requiring ship and port facility security plans based upon security assessments; and requiring training, drills and exercises to ensure familiarity with security plans and procedures.

Government and shipping company responsibilities

Contracting Governments are responsible for setting the applicable security level; approving port facility security assessments; determining which port facilities will be required to designate a port facility security officer; approving a port facility security plan and subsequent

[1] Maritime Programme Coordinator, Secretariat of the Pacific Community; JohnPH@spc.int
[2] Fisheries Development Adviser, Secretariat of the Pacific Community; LindsayC@spc.int

amendments to an approved plan; implementing control and compliance measures pursuant to regulation XI–2/9 (amendments to SOLAS); and establishing the requirements for a declaration of security. There are specific responsibilities that cannot be delegated to a recognised security organisation.

Shipping company responsibilities include ensuring the ship security plan contains a clear statement emphasising the master's authority, as well as provisions needed to support the company security officer and the ship security officer in carrying out their duties.

Ship and port security

Both the ship and port facility security sections of the ISPS Code contain requirements and guidance for: security assessments, security plans, records (a paper trail), responsibilities of the port facility security and ship security officers as well as training, drills and exercises with regard to security on either the ship or the port facility.

The Code defines three security levels. Level 1 is the level at which ships and port facilities normally operate, and defines the minimum appropriate protective security measures that should be maintained at all times. Security level 2 corresponds to a heightened risk of a security incident (for which additional protective security measures are required); level 3 is used for an exceptional security risk (a security incident is probable or imminent). Apart from ensuring that all ship security duties are performed, the Code contains provisions regarding the control of access to ships, the control of embarkation of persons and their effects, and the monitoring of restricted areas, deck areas and areas surrounding ships. Additional sections address supervising the handling of cargo and ships' stores, plus ensuring that security communication is readily available.

Part A of the ISPS Code details port facility security requirements to be implemented at various security levels; guidance for extra precautions is provided in Part B. Activities include ensuring that all port facility security requirements are implemented; controlling access to port facilities; monitoring port facilities, including anchorage and berthing areas; monitoring restricted areas; supervising the handling of cargo and ship's stores; and ensuring that secure communication is readily available.

Verification and certification

Ships are subject to security verification, which serves as the basis for issuance of an international ship security certificate. Certificates are valid for not more than five years, and at least one intermediate verification must take place during this time. Flag States are responsible for verification, but this can be delegated to a recognised security organisation.

Part B of the ISPS Code contains very useful advice on the implementation of Part A. Although for guidance only, it is prudent if those responsible for security policies implement Part B recommendations as far as possible.

Can the ISPS Code be applied to fishing vessels?

The 1974 SOLAS Convention specifies the classes of ships to which the ISPS Code applies; these do not include fishing vessels. Nothing prohibits a State from requiring that a fishing vessel flying its flag comply with some or all of the provisions of the ISPS Code, however.

There are over 1000 foreign and several hundred domestic fishing vessels of all classes currently fishing in the Pacific region. The broad policy question is not whether these vessels should be subjected to some form of security regime, but how such a requirement can be administered and enforced. From a legal perspective, security issues fall outside coastal States' fisheries management and enforcement powers; consequently, it would seem out of order to expect PICTs to evoke their fisheries powers to require all fishing vessels to have a ship security system in place. The practical and logistical difficulties that PICTs could face if such a requirement were to be made mandatory would be onerous.

The nature of fisheries presents logistical problems. There is no consistency in how fishing vessels are licensed. Some foreign fishing vessels are licensed as members of an association, with which individual PICTs have standing access agreements. In such instances, the licence and registration applications for the various vessels are undertaken by the association, whose headquarters might be in Tokyo, Kaoshung, or Seoul. These applications are generally submitted simultaneously. The vessels are usually on the fishing grounds, and licences are normally issued to foreign fishing vessels without any physical inspection. It does not make sense, either logistically or economically, to require foreign fishing vessels to enter port before they can be licensed, as most do not make port calls, and have the capacity to spend months at a time at sea before they unload their catch.

Other foreign fishing vessels may be licensed directly by the fisheries departments, but never make any port calls. A third category of foreign fishing vessels operating in the region includes locally based foreign fishing vessels, which usually have an

arrangement with a PICT to be based locally and to land all their catch in that country. Some of these vessels operate under charter to local fishing companies. Although these vessels fly foreign flags, their operations are conducted wholly within the region. Other locally based foreign fishing vessels may take up the flag of the country they are operating from as part of the licensing requirement. Regardless of vessel's flag, the highly mobile and migratory nature of the fishing industry would present immense logistical problems for enforcing the ISPS Code, if the Code was applied to all fishing vessels.

Legally, it may be outside the ability of PICTs to impose such a requirement since the IMO has specifically stated that the Code does not apply to fishing vessels, even though the State whose flag the fishing vessel flies may require their vessels to have a ship security system. It is not clear, therefore, what the legal position would be if PICTs required foreign fishing vessels in the region to have a ship security system. It might not be opposable to the Flag States, as they could argue that legally they are the only competent authority that could require fishing vessels to have a ship security system. This raises an issue: how can the Code be practically applied, in a way that Flag States could not oppose. Some PICTs have already included fishing vessels in their security regulations, but this only applies to vessels flying their flag; furthermore, the requirement is not enforced.

Obviously, there are legal and practical issues that must be considered before the ISPS Code can either be applied directly to fishing vessels, or adapted in some way to address fishing vessel security. In addition to the fundamental legal question of whether application of the code to fishing vessels would not be tantamount to a breach of the Code (insofar as unilateral application of the ISPS Code to fishing vessels would violate the Code's exemption), it should be determined whether a more stringent Code could be developed for the region. Factors to be taken into account in determining whether more stringent measures need to be applied to fishing vessels in the region are the scale of the threat that fishing vessels pose, and more importantly, whether the IMO would sanction such measures. Finally, there is also the issue of whether the IMO has jurisdiction over fishing vessels. In addressing these questions, it is important to determine what is currently being done to address security or criminal concerns.

It would appear that the fisheries provisions on the Law of the Sea Convention do not grant States the power to require foreign fishing vessels to have a ship security system, because this is not a matter that relates to fisheries management and conservation. Consequently, coastal States would have to exercise their general maritime and security powers as a means of requiring fishing vessels to be subject to security checks in port. Under such an option, PICTs could enhance their port State powers (already granted under the Code) and extend these to include fishing vessels as a matter of course.

Conclusions

As outlined above, the application of IMO security measures to fishing vessels, as these currently stand, suffers from legal and practical difficulties. The ISPS Code is specifically designed to cover security in regard to terrorism or terrorist threat, whereas the main concerns relating to fishing vessels appear to be in regard to piracy, the smuggling of people and/or illegal goods (drugs, firearms, alcohol, etc.), and stowaways, which are not primarily terrorism-related issues.

An additional complication is the lack of consistency in how PICTs licence fishing vessels, and the differences that exist between PICTs in terms of their national legislation addressing fishing vessels, and how vessels are addressed. In order to address these issues (and to avoid loopholes whereby fishing vessels move to a particular country or territory in the region where requirements are less stringent), a consistent regional approach to fishing vessel security should be taken. This approach could examine ways to include fishing vessels under the ISPS Code, or examine development of a separate arrangement that addresses the issue consistently across the region. Regardless of which approach is adopted, stakeholder participation will be essential in the development of a regional approach; this should include the maritime and fisheries departments in each PICT and their respective industries, so as to ensure that a workable, cost effective arrangement can be agreed upon.