



# INTERNATIONAL ASSOCIATION OF PORTS AND HARBORS (IAPH)

5<sup>th</sup> Floor, North Tower New Pier Takeshiba  
1-11-1 Kaigan, Minato-ku, Tokyo 105-0022, Japan  
Tel: +81-3-5403-2770 Fax: +81-3-5403-7651  
E-mail: [info@iaphworldports.org](mailto:info@iaphworldports.org) Web site: <http://www.iaphworldports.org>

## Port and Maritime Security

### IAPH Policy and Guidance Paper

(Revision 23 April 2002)

#### 1. Introduction

The world in which we live and conduct our business is subject to rapid change. Globalisation and liberalisation of trade accelerate that process. Open frontiers lead to less involvement and control of regulatory authorities and all elements in the logistic chain can be potential targets for illegitimate organizations.

However, since the tragic events of September 11, 2001 consideration has also to be given to the use of ships and their cargoes as potential terrorist weapons. There is consequently a need to re-assess existing ship and related port security plans to address potential terrorist activities. This is all the more important in view of the economic importance of most ports for their national economy.

Ship security is the responsibility of international organizations such as the International Chamber of Shipping, ICS, and proposals to that effect have been prepared by them.

Port security is first and foremost a responsibility for the Port Authority and an issue which is dealt with in IAPH. Ports differ widely in their characteristics, lay-out and vulnerability and it is therefore not practical to develop detailed and uniform standard comprehensive port security plans. However, IAPH believes that it is possible to develop generic guidelines for port authorities from which specific issues can be selected to address in respect to each port, to a greater or lesser degree, threats applicable to them. This paper provides guidance on these issues.

To be effective, it is very important that ship and port security plans can be dovetailed together to form a comprehensive set of security measures relevant to the specific location. Guidance thereon is contained in the joint ICS/IAPH submission to IMO.

Port authorities are usually the main orchestrator of their port as a logistic nodal point and as such they can provide a valuable contribution to the establishment of an integral port and maritime security policy.

Such a policy should address the source of the potential threats as well as minimization of the effects. The approach can be visualised as follows:

Sensitization → Pro-action → Prevention → Preparation → Repression → After care

## **2. Port security policy**

The ports security policy should be developed in close co-operation of all the authorities involved. Its main characteristic is that it addresses two main elements: the port area as a whole and the individual companies operating in the port.

### **1. Multi-disciplinary (overall) Port Security Plan**

The overall port security plan can be considered to be the scenario, describing all measures that need to be taken with regard to the security of the port as a whole. Apart from a description of the measures and the facilities available for these measures, it should also contain a description of the division of responsibilities of the different actors.

The plan should address all the elements of the security chain, from sensitization initiatives (creating awareness) to the actual organization of incident combating and cyclic policy review. It is essential that the overall co-ordination rests with a Port security Committee in which all relevant authorities closely co-operate. These may differ from country (port) to port, but they will almost always include the Port Authority, Police, Justice department, Customs, Fire brigade, medical services and the environmental department. It is also imperative that this Port security Committee works closely together with the local port industry.

That co-operation is necessary for creating awareness and involvement and to mutually develop security toolkits.

### **2. Port Facility Security Plans**

As said, the overall Port Security Plan requires the active involvement of the local port industry. Through that co-operation generic guidance should be developed for the individual port facilities,

terminals, industries etc., so as to enable these to develop their own custom made Facility Security Plan. Such a plan should contain measures to increase the alertness of personnel, to counter criminal infiltration of the organization, secure the company area and its installations. It should also pay attention to procedures for calamities, information supply, communication and education and training of personnel.

### **3. Essential conditions for a successful port security plan**

The approach as described before requires a number of essential conditions in order to be successful.

- Awareness among all relevant partners, authorities and private enterprise
- Vulnerability assessment
- Knowledge, experience in security matters
- Co-operation
- Information management
- Communication

### **4. Awareness**

In the introductory paragraphs it is argued that ports are susceptible to criminal activities, including acts of terrorism. However, experience shows that in general, this is not experienced as such in the average port industrial community. As a result, there is no or insufficient basis for initiating activities, investing funds and co-operating with other actors. For that reason it is necessary to develop a programme aimed at creating awareness among the industry by explaining the various potential threats, in terms of calamities as well as economic damage.

### **5. Vulnerability assessment**

It will be clear that the measures described in the Port or Facility Security Plan should be directed at those areas where they are likely to have the maximum effect. For an effective security approach it is therefore essential that risk analyses are conducted both at overall port level as well as on individual port facility level. Weak spots, both in a physical sense as well as in an organizational sense should be made visible through the analysis process. Vulnerability assessments should be carried out at regular intervals and be part of the management process of the port or the port facility.

### **6. Knowledge and experience**

Knowledge and experience in security issues are essential elements for a successful approach. These elements are usually not available at individual company level. By establishing a Knowledge Centre in

which all relevant authorities co-operate, and make their knowledge and experience available to the local port industries, this deficiency can be remedied. Such Knowledge Centre may also serve as central platform for addressing complex security issues and could also facilitate education and training of port facility personnel. Obviously care should be taken at securing the integrity of the information handled through the Knowledge Centre.

## **7. Co-operation**

The nature of port security is very complex and it therefore requires close and intensive co-operation between all actors involved. This will range from local co-operation between the port industry and authorities to international co-operation between authorities and ports and port organizations. In this context co-operation between the service providers in the port should be addressed. These service providers are often the first to personally contact the ship and its crew. Pilots, tug boat companies, linesmen and suppliers of other services such as drinking water and bunkers, should be trained in identifying potential danger and in ways how to handle such situations.

## **8. Information management**

An effective security system requires high quality information and information exchange. Accurate and timely information is crucial for the identification of potential threats and for taking the proper counter measures. It is necessary to lay the responsibility for information collection, interpretation and dissemination with an experienced organization such as the police. This focal point should maintain close contact with relevant national authorities as well as local parties in the port area, both authorities and industry.

## **9. Communication**

Proper and unambiguous information to the relevant parties, including the population in areas adjacent to the port is of importance in order to create a firm basis for the measures to be taken. A communication plan should therefore be part of the Port Security Plan. At regular intervals the population should be informed about security projects without endangering the integrity of these plans by disclosing sensitive details.

## **10. Preventive measures**

Preventive measures must be taken on the basis of local circumstances. They are aimed at protection of the port and its industrial complex as well as persons on board (passengers and crew) and ashore (port personnel and inhabitants of nearby living quarters).

## **11. Cargo inspections**

Cargo inspections aimed at identifying weapons, drugs, explosives and other matters of a threatening nature. Rather than inspect cargo at random, inspections should be targeted. Targets will be established on the basis of document checks in combination with a system of risk analysis. This will enhance the probability that targeted cargo proves to be non-compliant with regulations or to contain contraband.

Since containers are considered to be most susceptible to criminal activities, special attention should be paid to containerised cargo. Suitable equipment is X-ray machines, portable detection equipment and sniffer dogs.

In order not to disturb the logistic process in an unacceptable manner, the number of physical checks should be carefully chosen. Percentages will differ from port to port, but experience has shown that even a limited percentage, coupled with a targeted approach based on risk analysis, can provide an acceptable security level.

## **12. Identification check of passengers and crews**

In most cases the responsibility for checking the identification of both crews and passengers rests with the seaport police or the immigration authorities. For passengers this will involve a passport check. For crew members an identity card based on the provisions of ILO will serve as a suitable identity document.

## **13. Identification check of port personnel**

For personnel engaged in the port industry this issue should be part of the facility or industry security plan.

For personnel engaged in security enforcement:

To be developed.

## **14. Integration with Maritime Security**

A Port Security Plan is not enough to guarantee security and reliability throughout the total logistic chain, including the hinterland of the port and the sea transport. To that end, similar measures as described above, need to be developed for the individual links throughout the logistic chain.

## **15. Concluding remarks**

Regarding sea transport, including the immediate ship/shore interface IMO is presently developing international regulations that should be endorsed at a diplomatic conference in November or December 2002. It will be essential that regulations relating to maritime security dovetail with port and port facility security plans. Close co-operation of all international actors is necessary to ensure the establishment of effective measures to ensure maritime security both at sea as well as in ports and their hinterland.

IAPH is dedicated to play an active role in this process. This document should provide the basis for generic guidance for ports to develop their own custom made security plans based on their particular characteristics.

Abu Dhabi, 23 April 2002