INTERNATIONAL STANDARD

ISO 20858

First edition
2007-10-15

Ships and marine technology — Maritime port facility security assessments and security plan development

Navires et technologie maritime — Évaluation de la sécurité des installations portuaires maritimes et réalisation de plans de sécurité

Reference number
ISO 20858:2007(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 20858 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*.

This first edition of ISO 20858 cancels and replaces ISO/PAS 20858:2004, which has been technically revised.

Introduction

This International Standard addresses the execution of marine port facility security assessments, marine port facility security plans (including countermeasures) and the skills and knowledge required of the personnel involved. This International Standard is designed to ensure that the completed work meets the requirements of the International Maritime Organization (IMO) International Ships and Port Facility Security Code (ISPS) and the appropriate maritime security practices that can be verified by an outside auditor. Since other ISO standards may address non-marine port facilities the word “marine” usually appears before port facilities in this standard. This standard is intended to address port facilities as defined in the ISPS.

Ships and marine technology — Maritime port facility security assessments and security plan development

1 Scope

1.1 General

This International Standard establishes a framework to assist marine port facilities in specifying the competence of personnel to conduct a marine port facility security assessment and to develop a security plan as required by the ISPS Code International Standard, conducting the marine port facility security assessment, and drafting/implementing a Port Facility Security Plan (PFSP).

In addition, this International Standard establishes certain documentation requirements designed to ensure that the process used in performing the duties described above was recorded in a manner that would permit independent verification by a qualified and authorized agency (if the port facility has agreed to the review). It is not an objective of this International Standard to set requirements for a contracting government or designated authority in designating a Recognized Security Organization (RSO), or to impose the use of an outside service provider or other third parties to perform the marine port facility security assessment or security plan if the port facility personnel possess the expertise outlined in this specification. Ship operators may be informed that marine port facilities that use this document meet an industry-determined level of compliance with the ISPS Code.

Port infrastructure that falls outside the security perimeter of a marine port facility might affect the security of the facility/ship interface. This International Standard does not address the requirements of the ISPS Code relative to such infrastructures. State governments have a duty to protect their populations and infrastructures from marine incidents occurring outside their marine port facilities. These duties are outside the scope of this International Standard.

1.2 Conformance

While compliance with the ISPS Code is internationally mandated for all signatory countries, the use of this International Standard is voluntary. If a contracting government establishes requirements that preclude the use of this International Standard, local law takes precedence and compliance with this International Standard should not be claimed.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
cargo
items that are placed on the ship to be transported to another port, such as boxes, pallets, cargo transport units, and bulk liquid and non-liquid matter

2.2
consequence
loss of life, damage to property or economic disruption, including disruption to transport systems that can reasonably be expected as a result of an attack on or at the marine port facility

2.3
International Maritime Organization
IMO
specialized agency of the United Nations whose purpose is “to provide machinery for cooperation among governments in the field of governmental regulation and practices relating to technical matters of all kinds affecting shipping engaged in international trade; to encourage and facilitate the general adoption of the highest practicable standards in matters concerning maritime safety, efficiency of navigation, and prevention and control of marine pollution from ships”

2.4
ISPS Code
international code for the security of ships and port facilities consisting of Part A (the provisions of which shall be treated as mandatory), and Part B (the provisions of which shall be treated as recommendatory), as adopted on 12 December 2002 by Resolution 2 of the Conference of Contracting Governments to the International Convention for the Safety at Sea, 1974, as may be amended by the Organization

2.5
likelihood
probability of a threat scenario becoming a security incident, considering the resistance the physical and operational security measures in place at the marine port facility

2.6
management system
organization’s structure for managing its processes or activities that transform inputs of resources into a product or service, which meet the organization’s objectives

NOTE It is not the intent of this document to specify a specific management system or require the creation of a separate security management system. ISO 9001 (Quality Management Systems), ISO 14001 (Environmental Management Systems), ISO 28000 (Supply Chain Security Management Systems) and the International Maritime Organization’s International Safety Management (ISM) Code are examples of management systems.

2.7
marine port facility
those areas of the port and harbour where the ship/port interface takes place

NOTE The ship/port interface means the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons and/or goods, or the provisions of port services to and from the ship. This includes areas such as anchorages, waiting berths, and approaches from seaward. The marine port facility extends landside to the security perimeter. Note that, for the purposes of this International Standard, there can be more than one marine port facility in a harbour. In that case, only the anchorages, waiting berths, and approaches from seaward that are used to service the marine port facility using this document are included. There can be areas of ports and harbours that are addressed in the ISPS Code, but that are not addressed in this International Standard.

2.8
Port Facility Security Plan
PFSP
plan to ensure the application of measures designed to protect the people, port facility, ships, cargo, cargo transport units, and ship stores within the port facility from the risks of a security incident

2.9
risk
chance of injury, damage or loss postulated by considering the consequence of a threat and the likelihood of its occurrence

2.10
security
resistance to intentional, unauthorized acts designed to cause harm or damage to ships and ports

2.11
security crisis management team
group of people who have the knowledge and authority to bring the necessary resources to bear in the event of an imminent security threat or actual security incident

2.12
security incident
suspicious act or circumstance threatening the security of a ship or port facility

2.13
security personnel
individuals who have assigned security duties defined in the port facility and who may or may not be employees

2.14
ship's stores
supplies and spare parts intended for use by a ship calling on a marine port facility

2.15
target
personnel, ships, cargo, physical assets, and control/documentation systems within a marine port facility

2.16
security threat scenario
means by which a potential security incident might occur

NOTE Because attack methods are nearly infinite, several general postulated security threat scenarios are specified to address the full range of attack scenarios. Local authorities, port facility management and personnel conducting the security assessment could add more specific security threat scenarios to the list of general security threat scenarios, depending on local circumstances.

3 Performance of the security assessment

3.1 Overview of the security assessment

The port facility implementing this International Standard shall conduct a security assessment or draw upon existing security assessments that are valid, documented and meet the requirements of this International Standard. The assessment shall consider security threat scenarios, consequences of a successful attack on the port facility, and the likelihood of each security threat scenario being successful given the security measures in place. Based on these considerations, a determination shall be made if additional security countermeasures are required.

NOTE The authorized maritime security group convened to compose the PFSA needs to be collectively knowledgeable in port/facility operations, security and the potential security threats that could occur at the specific site. From their experience and training, they review current conditions (using a provided Performance Review) and produce a realistic list of security threat scenarios that could adversely affect the facility. These potential security incidents are thoroughly studied, and then charted with regard to the likelihood of an occurrence and subsequent consequences, if it occurs. The resultant security risk chart for each of these incidents indicates which are of such gravity as to need effective human and/or physical countermeasures. The formulating team will increasingly apply these countermeasures until the identified risk is reduced to an acceptable level (meeting with the approval of the contracting government).

At this stage, the PFSA evolves into the PFSP. The aforementioned process is dealt with in more detail within this document, and forms the route toward a site-specific facility plan. Although basically stated, nothing here is intended to oversimplify the effort needed to construct a comprehensive quality plan. The above sequence will establish a plan for effective security for the standard Security Level 1, following which the group will reapply the countermeasures required for the higher Security Levels 2 and 3, as described herein. The contracting government reviews and approves the prepared plan for submission to the IMO.

3.2 Personnel conducting the security assessment

Those involved in a Port Facility Security Assessment (PFSA) shall be able to draw upon expert assistance relative to:

— knowledge of current security threats and patterns;

— recognition and detection of weapons, dangerous substances, and devices;

— recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

— techniques used to circumvent security measures;

— methods used to cause a security incident;

— effects of explosives on structures and port facility services;

— port business practices;

— contingency planning, emergency preparedness, and response;

— physical security measures (e.g. fences);

— radio and telecommunications systems, including computer systems and networks;

— transport and civil engineering;

— ship and port operations;

— maintenance of appropriate measures to avoid unauthorized disclosure of, or access to, sensitive security material;

— knowledge of the requirements in Chapter XI-2 and part A of the ISPS Code and relevant national and international legislation and security requirements;

— knowledge of security and surveillance equipment and systems, as well as their operational limitations.

All personnel involved in a PFSA, including those called on to provide the expertise listed above, shall be listed in the Port Facility Security Assessment Report as specified in 6.2.

4 Security assessment procedures

4.1 General

A security assessment provides the basis for developing the Marine Port Facility Security Plan. The methodology used in the assessment is not specified in this International Standard. However, the methodology used in the assessment shall meet the requirements of this International Standard.

4.2 Scope of the security assessment

The scope of the assessment extends to those port facilities and port infrastructures that could be threatened or be used to threaten maritime trade.

The port facility security assessment shall include, as a minimum, all areas

— where port facility/ship operations are conducted within the port facility,

— where cargo is staged, stowed or handled before/following marine transportation within the port facility,

— where cargo documentation for marine transportation is handled/accessible within the port facility,

— attached to the port facility without an intervening security perimeter, and

— including ship channels used to approach the port facility.

4.3 Current status of security at the port facility

The person(s) conducting the security assessment shall review all current security operations and emergency plans used by the port facility. All reviewed plans shall be listed. The person(s) conducting the security assessment shall, in addition, conduct an on-site review of the port facility and surrounding vicinity. As a minimum, the person(s) conducting the security assessment should examine and document items in the following performance review list during the port facility security assessment.

This performance review list is not exhaustive. Some items on the list are not applicable to certain port facilities and a negative indication concerning any specific factor does not mean that security is inadequate. The performance review list is a generalized method for assessing the current status of a port facility's security; it is not intended to set security requirements.

A copy of the completed performance review list shall be included in the assessment report.

In Table 1, if the factor indicated is in effect at the port facility, the "yes" block should be checked. If the factor is not in effect, the "no" block should be checked. If the factor is not applicable, put "NA" in the "Comments" column (additional comment pages may be added as needed).

Table 1 — Performance review list

Factors		Yes	No	Comments
Do the current port facility security documents address the following?				
1	Security organization of the port facility			
2	Organization's links with other relevant authorities and the necessary communication systems to enable an effective, continuous operation of the organization and its links with others, including ships in port			
3	Basic Security Level 1 measures, both operational and physical, that will be in place			
4	Additional security measures that will enable the port facility to progress without delay to Level 2 and, when necessary, to Level 3			
5	Regular reviews or audits of the PFSP or its amendments in response to current experiences or changing circumstances			
6	Reporting procedures, including lists of appropriate contracting government's contact points			
7	Role and structure of the port facility security organization			
8	Duties, responsibilities and training requirements of all port facility personnel who have security roles, and the performance measures needed to assess their effectiveness			
9	Port facility security organization's links with other national or local authorities with security responsibilities			
10	Communication systems provided to enable effective and continuous communication among port facility security personnel, ships in port and, when appropriate, with national or local authorities with security responsibilities			

	Factors	Yes	No	Comments
11	Procedures or safeguards necessary to enable such continuous communications to be maintained at all times			
12	Procedures and practices to protect security-sensitive information held in paper or electronic format			
13	Maintenance frequency of security equipment and procedures to assess the continuing effectiveness of security measures and equipment, including identification of, and responses to, equipment failures or malfunctions			
14	Procedures that require submission and assessments of reports relating to possible breaches of security or security concerns			
15	Procedures relating to traffic flow within the facility			
16	Procedures covering the delivery of spare parts and ship's stores			
17	Procedures to maintain and update records of dangerous goods and hazardous substances, including their location within the port facility			
18	Means of alerting and obtaining the services of waterside patrols and specialist search teams, including bomb searches and underwater searches			
19	Procedures for assisting ship security officers in confirming the identity of those seeking to board the ship when requested			
20	Procedures for facilitating shore leave for ship personnel or personnel changes, as well as access of visitors to the ship (including representatives of seafarers, welfare and labour organizations)			
21	Procedures for internal and external notifications for the following (if applicable): — bomb/terrorist security threats; — an actual explosion or detonation; — fire on the port facility or berthed ship; — hostage situation; — civil disturbance/violent labour dispute; — emergency evacuation; — informing employees to/not to report to work; — accounting for all personnel on the port facility, including their names; — specific safety guidance on the proper use of fire arms by authorized personnel in the port facility.			
22	Sketches of the port facility, access points, working areas, cargo stowage areas			
23	Security organization of the port facility			
Are the following true for the organization and performance of port facility security duties?				
24	Security force is as described in the PFSP's "Security Force" and is adequately equipped with vehicles to patrol, respond to alarms and emergencies and maintain supervision			
25	Personnel with security roles or access to restricted areas have passed background checks performed at the time of employment and periodically thereafter. This has been documented and the process used explained			
26	Security personnel are provided with security updates at the beginning of each work shift			
27	Security force orders are reviewed monthly and revised as needed			
28	Security personnel wear distinct/authoritative uniforms			

	Factors	Yes	No	Comments
29	Security personnel patrols routinely cover all portions of the port facility, including all exterior and principal interior access points			
30	Port facility has an organized/equipped security crisis management team or local community has an organized/equipped crisis management team			
31	Procedures are in place to bring in additional security in an emergency or crisis situation			
32	Liaison has been established between the port security officer and local government			
33	Security personnel report their status to a designated contact during their security patrols			
34	Security personnel assignments and patrol times and routes are varied to prevent predictability			
35	Training records for security personnel are maintained			
36	Armed security personnel are properly trained in the use of force and weapons and certified by appropriate authorities			
37	Vehicles intended for use in security patrols are conspicuously marked			
38	Only approved personnel are allowed to carry firearms			
39	Security force inspects security barriers and clear zones at least monthly			
40	Records of security inspections are maintained and accessible to authorized personnel			
41	If fitted, intrusion detection system signals are monitored at a central location and a security response can be initiated from that point			
42	All external access points are guarded or secured and locked when not in use			
43	Security measures are in effect to protect electrical power supplies and transmission facilities. (If equipped with an emergency generator, it should be within a restricted area.)			
44	Security measures are in effect to protect communications systems			
45	Non-compliance with the security plan is noted and remedial action is promptly taken			
46	Security measures are in place where water bodies form part of the perimeter barrier to prevent/detect illegal unauthorized access			
47	Port facility has effective after-hours/weekend restricted area security checks			
Access to the port facility				
48	Perimeter fencing is adequate to prevent unauthorized entry and meets recognized industry standards or government standards (explain which standard)			
49	If masonry or brick walls form part of the perimeter barrier, they are inspected regularly for effectiveness			
50	Buildings, floors or roofs that form part of the perimeter barrier are complemented by intrusion-detection equipment			
51	Perimeter fences/walls have unobstructed zones on each side			
52	Access points through the perimeter are kept to the minimum needed for safe and efficient operations			
53	Gates provide equivalent level of security as perimeter fencing			
54	Pass system is used to identify all personnel entering the port facility and indicate their degrees of access to portions of the port facility			

Factors		Yes	No	Comments
55	Employees display passes when working in restricted areas			
56	Security personnel certify passes of bearers upon entry			
57	Personnel pass system is managed to prevent unauthorized issuance of passes			
58	Lost passes are replaced with passes bearing different serial numbers			
59	Passes are designed to enable security and other personnel to recognize individuals quickly and positively identify the authorizations and limitations applicable to the bearer			
60	Pass procedures cover the resolution of queries by the pass checker			
61	Procedures ensure the return or disablement of passes upon termination of employment or assignment			
62	Procedures are in place to control the whereabouts of visitors			
63	Procedures are in place to provide security for the port facility to meet international agreements on the humane treatment of ship crews			
64	Truck drivers, vendors and other visitors are permitted access only to those areas required to conduct their business; only authorized personnel are permitted in warehouses			
65	Permanent records of visitors, vendors, and truck drivers entering the port facility are maintained and easily accessible by authorized personnel for a defined period			
66	Random screening (at a minimum) of trucks for explosives and weapons are made of vehicles entering the port facility			
67	If parking is allowed on the port facility, access to parking areas is supervised and restricted by a pass system for all vehicles			
68	Parking-pass records that match personnel with pass number and motor vehicle identification are maintained			
69	All vehicles are required to be parked in designated parking areas. Employees, vendors and visitors going to or from parking areas are required to pass through an area under the supervision of security personnel			
70	Parking for employees, dockworkers and visitors is at away from docks, wharfs and piers, and outside of fenced operational, cargo handling, and designated storage areas			
71	Temporary parking passes are issued to vendors and visitors for parking in designated areas			
72	All openings that permit access to the port facility (such as drainage ditches, tunnels, manholes for sewers and utility access, and sidewalk elevators) are properly secured			
Restricted areas within the facility				
73	Restricted areas of the port facility have been designated in the port security plan by the port facility operator			
74	All restricted-area access points are appropriately posted			
75	All restricted areas have clearly marked perimeters			
76	All restricted areas have pass systems and entrances and exits are guarded, controlled, or closed and secured			
77	Only those personnel whose duties require access to information or equipment are allowed within restricted areas			
78	Security personnel perform routine patrols of restricted areas			

	Factors	Yes	No	Comments
79	At Security Level 2, procedures are in place to — enhance the effectiveness of barriers or fencing surrounding restricted areas by using either patrols or automatic intrusion-detection devices, — reduce the number of access points to restricted areas and increase the controls applied at the remaining accesses; restrict parking adjacent to berthed ships, — increase supervision of personnel and cargo movement/storage in the restricted areas, — continuously monitor and record surveillance equipment, — enhance the number and frequency of patrols, including waterside patrols undertaken on the boundaries of restricted areas and within those areas, — establish and restrict access to areas adjacent to restricted areas, and — enforce restrictions on access by unauthorized craft to the waters adjacent to ships using the port facility.			
80	At Security Level 3, procedures are in place to — set up additional restricted areas within the port facility in proximity to the security incident or potential location of the security threat to which access is denied, and — prepare for the searching of restricted areas as part of a search of all, or part, of the port facility.			
Handling of cargo				
81	The port facility has measures in place that — prevent cargo tampering, and — prevent cargo that is not meant for carriage from being accepted and stored within the port facility.			
82	Security measures in place include inventory-control procedures at access points to the port facility, once cargo within the port facility has been identified as having been checked and accepted for loading onto a ship or for temporary storage in a restricted area while awaiting loading. Cargo that does not have a confirmed date for loading is clearly identified as such, segregated from cargo to be loaded or is prohibited from the port facility			
83	At Security Level 1 — cargo, cargo transport units and cargo storage areas are routinely checked within the port facility prior to and during cargo handling operations, — checks are performed to ensure that cargo entering the port facility matches the delivery notes or equivalent cargo documentation, — vehicle screenings for explosives and weapons are conducted, and — when cargo enters the port facility, and upon storage there, checks are conducted of the container seals that are used to prevent tampering.			
84	Restricted areas are designated for the safe inspection of cargo			
85	Cargo stored in open areas near a fence or port facility perimeter shall be spaced to enable security personnel to see between the perimeter barrier and the cargo, to minimize the use of stacked cargo to transit over the perimeter barrier			
86	Cargo stored in warehouse facilities is properly stacked and placed so that security personnel may observe it. (This will minimize areas where people can hide)			
87	Cargo information and delivery orders for cargo, cargo transport units, and containers are checked for accuracy and verified before acceptance			

	Factors	Yes	No	Comments
88	Access to areas where documentation is processed is limited to authorized personnel; ship documents are safeguarded from theft and documentation fraud			
89	The placement of cargo on the port facility is controlled and all cargo can be readily identified by security and management personnel			
90	Drivers entering the port facility are issued gate passes to control and identify those authorized to pick up or deliver cargo			
91	Cargo is only released to drivers who have proper documentation and authorization			
92	Before receiving a shipment, personnel processing delivery orders verify the identity of the trucker and trucking company			
93	Cargo is moved directly from railcars or ships to storage facilities and directly from storage facilities to railcars and ships			
94	The master flow and drain valves, and valves that would permit direct outward flow of a bulk liquid or gas storage tank contents to the surface, are securely locked in the closed position when in a non-operating or non-standby status			
95	The starter controls on all bulk liquid and gas transfer pumps are locked in the “off” position, or located at a site accessible to authorized personnel only			
96	Loading and unloading connections of pipelines, loading arms, or transfer hoses are securely capped or blank-flanged when not in actual service or standby service			

	Factors	Yes	No	Comments
97	Security personnel are kept aware of locations of high-consequence and dangerous goods. The following is an indicative list of such goods: — Class 1, Division 1.1 explosives; — Class 1, Division 1.2 explosives; — Class 1, Division 1.3 Compatibility Group C explosives; — Class 1, Division 1.5 explosives; — Class 2.1, flammable gases in bulk; — Class 2.3, toxic gases (excluding aerosols); — Class 3, flammable liquids in bulk of packing Groups I and II; — Class 3 and Class 4.1, desensitized explosives; — Class 4.2, goods of Packing Group I in bulk; — Class 4.3, goods of Packing Group I in bulk; — Class 5.1, oxidizing liquids in bulk of Packing Group I; — Class 5.1, perchlorates, ammonium nitrate, and ammonium nitrate fertilisers, in bulk; — Class 6.1, toxic substances of Packing Group I; — Class 6.2, infectious substances of Category A; — Class 7, radioactive material in quantities greater than 3 000 A1 (special form) or 3 000 A2, as applicable, in Type B or Type C packages; — Class 8, corrosive substances of Packing Group I in bulk. NOTE 1 For the purposes of this list, “in bulk” means transported in quantities greater than 3 000 kg or 3 000 l in portable tanks or bulk containers. NOTE 2 For purposes of non-proliferation of nuclear material, the Convention on Physical Protection of Nuclear Material applies to international transport (supported by IAEA INFCIRC/225[Rev.4]). NOTE 3 For Class 7, A1 and A2 refer to maximum activity levels of radioactive materials. Specifically, A1 means the maximum activity of special-form radioactive materials permitted in a Type A package. A2 means the same for other than special-form radioactive materials. Special form means the material consists of materials of a certain minimum size (not likely to be distributed by wind).			
Delivery of ship stores, including a ship’s spare and replacement parts				
98	Drivers entering the port facility obtain gate passes to control and identify those authorized to deliver ship’s stores			
99	Procedures are in place to visually, physically or electronically/chemically inspect ship’s stores			
100	Procedures are in place to prevent tampering with ship’s stores			
101	Restricted areas are designated to perform inspections of ship’s stores			
102	Escorts are provided for delivery vehicles within the port facility where the PFSP requires it			
103	Ship’s stores are scheduled in advance of delivery and coordinated between the port facility and the ship			
104	Measures are in place to confirm that stores presented for delivery are accompanied by evidence that they have been ordered by, or are expected by, ship personnel			

Factors		Yes	No	Comments
Handling of unaccompanied baggage				
105	Security measures are in place which ensure that unaccompanied baggage (i.e. any baggage, including personal effects that are not with the passenger or member of ship's personnel at the point of inspection or search) is identified and subjected to appropriate screening for weapons and explosives before being allowed access to the port facility. Unaccompanied baggage shall be screened before it is transferred between the port facility and the ship, at any time that such baggage is left uncontrolled before being loaded onto a ship			
106	At security Levels 2 and 3, additional security measures are in place, including 100 % screening of all unaccompanied baggage for weapons and explosives			
107	Unaccompanied baggage or personal effects are segregated from cargo in a secured area			
108	Procedures are in place to restrict, suspend, or refuse to handle unaccompanied baggage			
Monitoring the security of the facility				
109	Illumination of the port facility is adequate to allow for the ready detection of unauthorized personnel and is free of shadowed areas in which an unauthorized person would not be detected. Illumination meets recognized industry or government standards (explain which standards)			
110	The perimeter of the port facility is illuminated, and continuous or standby lighting with automatic activation is acceptable			
111	The perimeters of all restricted areas are illuminated. (Continuous or standby lighting with automatic activation is acceptable)			
112	All open access points are illuminated			
113	All pedestrian entrances are illuminated. (Continuous lighting is required for all open pedestrian entrances. Pedestrian access points that are closed shall have standby or continuous lighting)			
114	All docks, piers, wharfs and other working areas are illuminated in a manner that does not interfere with navigation. (Continuous lighting is required when there is any activity in these areas. However, during times of inactivity, standby lighting is acceptable)			
115	All water approaches to dock, pier or wharfs are illuminated. (Continuous lighting is required when there is any activity in these areas. However, during times of inactivity, standby lighting is acceptable)			
116	All parking lots on the port facility are evenly illuminated in a manner that prevents shadows and areas of poor illumination between vehicles			
117	Protective perimeter lighting is arranged so that security force patrol personnel remain in comparative darkness			
118	The port facility has an emergency backup power source for its protective lighting system			
119	Lighting is provided from sunset to sunrise and during periods of low visibility			
120	The port facility uses an intrusion detection system (IDS)			
121	The controls for all intrusion detection/surveillance systems are secured with key locks or screws and equipped with tamper-proof switches			
122	There are alternative or independent power sources available for use on the system in the event of power failure			
123	The IDS is inspected and/or tested at least monthly			
124	The port facility security force has a reliable direct communication system between its designated security contact person and each security unit or post			
125	There is an alternative means of security communication available			

Factors		Yes	No	Comments
126	The designated security contact is in a physically secure location			
127	The communication system is capable of rapidly transmitting instructions to all security forces and confirmation of reception is provided			
128	All communications equipment is properly maintained			
Name or location of the port facility being reviewed:				
Name(s) of person(s) conducting the performance review:				
Date(s) of the review:				

4.3.1 Identification of assets and infrastructure

In addition to the security performance review list, the following information shall be documented and considered during the assessment.

— Those critical assets within or adjacent to the port facility that, if damaged, could threaten the operation of the port facility.

— Those assets adjacent to the port facility that, if damaged, could cause harm to the port facility or could be used to cause harm to the port facility.

— National or prominent symbols within, or adjacent to, the port facility that, if attacked, could affect the operations of the port facility.

— Areas that can be used for illicit observation of the port facility.

— Areas adjacent to the port facility that could be used for diverting attention from security of the port facility.

4.3.2 Consultations

Contact with local law enforcement and other appropriate government officials shall be attempted concerning:

— current and potential security threats to the port facility;

— any aspects of the port facility, including the ship traffic using the facility, that make it likely to be the target of an attack;

— consequences of loss of life, damage to property, economic disruption, including disruption to transport systems, of a port facility attack;

— the capabilities and intentions of those likely to mount such an attack;

— the types of possible attacks on the port facility.

The information received shall be documented and considered.

If the appropriate law enforcement and other government officials do not wish to participate in such a dialog, the organization should document their attempt(s) and state that appropriate law enforcement and other government officials did not participate at that time

4.4 Threat scenarios and security incidents

The methodology used to conduct a security assessment shall, as a minimum, identify the security threat scenarios listed in Table 2.

Table 2 — Application examples for security threat scenarios

Security threat scenarios	Application example
Intrude and/or take control of a target within the port facility and damage or destroy the target with explosives	Intruder plants explosives
Intrude and/or take control of a target within the port facility and damage or destroy the target through malicious operations/acts	Intruder takes control of a ship and runs it aground or intentionally collides with something, or intruder intentionally opens valves to release dangerous substances, etc.
Intrude and/or take control of a target within the port facility and create a hazardous or pollution incident without destroying the target	Intruder opens valves/vents to release toxic materials or releases toxic material brought along, or overrides interlocks leading to damage/destruction
Intrude and/or take control of a target within the port facility and take hostages/kill people	Goal of the intruder is to kill people
Externally attack the port facility by moving explosives adjacent to the target from the waterside, the shoreside or subsurface	Car/truck bomb is used to damage/destroy the port facility
Externally attack the port facility by ramming a stationary target with a ship or a land-based vehicle	Intentional collision meant to damage/destroy/block operations of the port facility. (NOTE: Evaluate overall consequences from the collision, but only evaluate the vulnerabilities of the target and not the vulnerabilities of the ship/vehicle used to ram the target)
Externally attack the port facility by launching or shooting weapons from a distance	Shooting at a target using a rifle, missile, etc.
Use the port facility as a means of smuggling illegal weapons or explosives into or out of the country Use the port facility as a means of smuggling people into/out of the country	Moving people into or out of the country, concealed in ship, containers or otherwise hidden on/in a ship/train
Cyber tampering by locally or remotely gaining access to facility's or ship's computer systems for the purpose of disrupting operations or facilitating illegal activities	Hacking into a port facility's cargo documentation files for the purpose of determining which containers have dangerous goods or weapons contained within them or Hacking into the computer system that is used to route cargo flow at a refinery for the purpose of intentionally overfilling storage tanks
Cargo tampering/sabotage to create a harmful situation	Adding reactive chemicals to products being shipped. Rigging the cargo to discharge while in transit. Weakening the cargo restraints or containers so that they fail while being moved or Changing the origin of a cargo to avoid/reduce the probability of government inspections in order to smuggle devices intended to cause destruction or Changing the classification of cargo that causes harm or damage
Unauthorized operations on a waterfront facility or ship other than those intended by management	Unauthorized personnel arranging to offload cargo at a waterfront facility from a ship without the knowledge of the waterfront facility management

4.5 Classification of consequences

An evaluation of consequences shall be conducted and shall consider potential loss of lives and economic losses. The contracting government may also specify that facilities of symbolic value and/or the threat to government installations be taken into account when evaluating the consequence of a security incident. The consequences of each security incident evaluated at a marine port facility shall be classified as high, medium, or low. If a numerical system is used in the assessment process, the numerical results shall be converted into a qualitative system. Rationales for the classifications of consequences for each security incident shall be documented.

NOTE 1 Care needs to be taken in establishing values of “high”, “medium” and “low” consequences. The use of excessively low threshold values could result in the requirement that countermeasures be considered for more threat scenarios than are needed. However, using excessively high threshold values may omit countermeasures for threat scenarios involving consequences that the port facility or nation cannot afford.

A “high” consequence classification could be considered as a consequence that would be unacceptable in all but low likelihood situations.

A “medium” classification of consequence could be considered as a consequence that would be unacceptable in a high likelihood situation.

A “low” classification of consequence could be considered as a consequence that is normally acceptable.

NOTE 2 Avoid confusing acceptability with desirability or approval. Rather, acceptability could be considered as a judgment of the amount of possible damage that a port facility or port state is willing to accept under certain conditions related to probability. A nation could determine that the possibility of a certain level of damage may be undesirable yet acceptable. The relative affluence of a port state can affect its acceptable threshold of consequences. A less affluent nation might be unable to recover from the same level of damage that a more affluent nation could, thus it would have a lower damage threshold. A more affluent nation could demand lower threshold values for issues because of public opinion, for example, potential damage to the environment. A developing nation might have to accept higher threshold values in spite of potential environmental damage.

4.6 Classification of likelihood of security scenarios

The status of physical and operational security measures in the supply chain as documented in the security performance review list and other documentation provided should be taken into account in classifying potential security scenarios. Physical security measures include objects that impede or detect unauthorized access to a target. Operational security measures include people and procedures that impede or detect unauthorized access to a target. The likelihood of each security scenarios becoming a security incident at a particular asset should be classified as high, medium and low.

— **High likelihood** should be used when the security measures in place offer little resistance to that security incident occurring. If a numerical system is used in the assessment process, the numerical results should be converted into this qualitative system.

— **Medium likelihood** should be used when the security measures in place offer moderate resistance to that security incident occurring.

— **Low likelihood** should be used in cases where the security measures in place offer substantial resistance to that security incident occurring.

The rationale for the classification of likelihood assigned to each security scenario should be documented.

4.7 Security incident scoring

Table 3 shows the security scenarios scoring chart shall be used to determine when countermeasures shall be considered for specific security scenarios.

Table 3 — Security scenarios

	Consequences			
Likelihood		High	Medium	Low
	High	Countermeasures	Countermeasures	
	Medium	Countermeasures		
	Low			

Identification of countermeasures is required for security scenarios that score: high in both likelihood and consequences: medium likelihood and high consequences; along with those scoring at high likelihood and medium consequences. Other security scenarios need not include countermeasures, unless they are considered advisable by the evaluator. The person assessing the security shall list each security scenario required to be considered for countermeasures.

4.8 Countermeasures

4.8.1 General

Using the methods specified in this document, each countermeasure shall be assessed for effectiveness in lowering the likelihood or consequences (or a combination of them) until the security scenario no longer requires that countermeasures be considered. The countermeasure achieving this is considered to be effective and shall be listed in the PFSP.

4.8.2 Countermeasure exceptions

If the contents of a sealed container or cargo transport unit are judged to present a risk requiring countermeasures according to the methodology used, the marine port facility is not required to establish countermeasures, unless the customs administration of the contracting government prescribes countermeasures. If no such measures are specified, the port facility shall notify their customs administration of the findings of their security assessment in regard to sealed containers. A statement that notification has been made shall be included in the Port Facility Security Assessment Report.

The IMO recognized the role of customs administrations in controlling the international movement of closed cargo-transport units (in Conference Resolution 9 attached to the SOLAS ISPS and entitled, “Enhancement of Security in Co-operation with the World Customs Organization [WCO] [Closed Cargo Transport Units]”) and requested measures to be developed. In response the WCO developed the SAFE Framework of Standards. If the contracting government implements these standards, they shall, where applicable, be incorporated into the port facility countermeasures list and security plan.

5 Port Facility Security Plan (PFSP)

5.1 General

A marine Port Facility Security Plan (PFSP) shall be developed to ensure the application of measures designed to protect the personnel, marine port facility, ships at berth, cargo, cargo transport units and ship’s stores/spare parts within the port facility from the risks of a security incident.

5.2 Prioritization of countermeasures

The countermeasures identified in 4.8 shall be implemented, in priority order, to achieve maximum benefit as judged by the port facility operator, unless the contracting government sets other priorities. Countermeasures selected for implementation shall be incorporated into the PFSP in the appropriate section.

5.3 Port Facility Security Plan contents

5.3.1 General

The items listed in 5.3.2 to 5.4 shall be incorporated into the PFSP.

5.3.2 Table of contents

A table of contents shall be provided, which at a minimum identifies all the items listed in 5.3.3 to 5.3.25 that are applicable.

5.3.3 Items in facility plot plan

The facility perimeters or areas covered by this security plan are as follows:

— all gates and access points (functional or otherwise);

— restricted areas on the port facility;

— ship berths;

— emergency equipment and emergency shutdown controls;

— parking areas;

— security checkpoints;

— building/structures within the facility;

— traffic flow, including emergency vehicle lanes;

— storage areas for dangerous materials (unless cargo is intermixed with non-dangerous materials, which should be noted);

— critical port facility assets.

5.3.4 Security administration and organization of the port facility

A description of the security organizational structure, including an explanation of duties and responsibilities of each person in the security organizational structure shall be provided.

A minimal breakdown of security duties should extend to the following levels:

— management;

— port facility security officer (PFSO);

— security personnel;

— personnel handling documentation related to cargo or ships' stores;

— any contractor with security duties.

5.3.5 Port Facility Security Officer

Provide the name of the Port Facility Security Officer (PFSO) and how the officer can be contacted at any time.

5.3.6 Changes in security levels

Define procedures for accomplishing the following.

— Ensuring that the facility operates in compliance with the required security level in effect for the port.

— Ensuring that all additional security requirements are being met, including notifying ships at berths and inbound when there has been an increase in the security level.

— At Security Levels 2 and 3, ensuring that the PFSO informs all port facility personnel about identified security threats, emphasizing reporting procedures and the need for increased vigilance.

5.3.7 Procedures for interfacing with ships

Define measures for interfacing with ships at all security levels.

5.3.8 Declaration of Security (DoS)

Define procedures for requesting a DoS and for handling DoS requests from a ship.

5.3.9 Additional requirements for port facility receiving passenger ship at Security Level 1

Define procedures taken prior to the arrival of a ship at the facility, in which the PFSO, master, and Ship Security Officer (SSO) (or their designated representatives) coordinate security needs and procedures while the ship is at the facility.

5.3.10 Communications

Define the means by which the PFSO can effectively notify facility personnel of changes in security conditions. The system shall allow effective and continuous communications among the port facility security personnel, ships interfacing with the facility, the PFSO and national and local authorities with security responsibilities.

At each active facility access point, a means of contacting police, security control or an emergency operations centre by telephone, cellular phone or portable radios (or equivalent means) shall be provided. Facility communications systems shall have backups for internal and external communications.

5.3.11 Security systems and equipment maintenance

Define procedures to ensure that the following requirements are met:

— security systems and equipment shall be in good working order and inspected, tested, calibrated and maintained according to manufacturers' recommendations;

— security system deficiencies shall be corrected promptly and the results recorded. Procedures for identifying and responding to security system and equipment failures or malfunctions shall be included.

5.3.12 Security measures for access control, including designated public access areas

5.3.12.1 Introduction

Define security measures to

— deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, ships, facilities or ports;

— secure dangerous substances and devices that are authorized by the appropriate authority to be on the facility;

— control access to the facility;

— identify authorized and unauthorized persons at any security level;

— allow temporary or continuing access for facility personnel and visitors, including seafarers' chaplains and union representatives, through the use of a badge or other system to verify their identities;

— allow certain long-term, frequent vendor representatives to be issued non-temporary passes that meet the requirements specified for employee passes;

— establish the frequency of application of any access controls;

— screen persons, baggage (including carry-on items), personal effects, and vehicles, including delivery vehicles, for dangerous substances and devices at the rate specified in the approved PFSP for Security Level 1;

— deter unauthorized access to the facility and to designated restricted areas within the facility;

— screen by hand, or with devices such as X-rays, all unaccompanied baggage prior to loading onto a ship;

— secure unaccompanied baggage in a designated restricted area, after screening, and maintain security control during transfers between the facility and a ship;

— require the checking of identification of any person seeking to enter the facility, including ship passengers and crew, facility employees, vendors, personnel duly authorized by the cognizant authority, and visitors;

— deny or revoke a person's authorization to be on the facility if a person is unable or unwilling to be identified or account for his or her presence. This procedure shall include methods of reporting this situation.

5.3.12.2 Additional security measures for access control, including designated public access areas

The PFSC shall define or establish procedures to address the following.

— Ensure that a system is established for checking the identification of facility personnel or other persons seeking access to the facility that identifies access points that shall be secured or attended in order to deter unauthorized access.

— Establish the means of identification required to allow access to the facility and for individuals and vehicles to remain on the facility without requiring challenges.

— Identify the locations where screenings of people, personal effects, and vehicles are to be conducted. The designated screening areas should be covered to provide for continuous operations, regardless of weather conditions.

— Identify locations within which restrictions or prohibitions that prevent unauthorized access are applied for each security level. Each location with means of access to the facility shall be addressed.

— Identify the types of restrictions or prohibitions to be applied and the means of enforcing them.

— Specify regular updating of the security plan.

— Define disciplinary measures to discourage violations of the security plan.

— Specify the conspicuous posting of signs that describe security measures in effect and clearly state the following:

- entering the facility is deemed as consent to screening or inspection;
- failure to submit to screening or inspection will result in denial or revocation of authorization to enter the ship.

— Designate restricted areas and provide appropriate access controls for these areas.

5.3.13 Security measures for access control, including designated public access areas at Security Level 2

Define additional security measures to be taken at Security Level 2.

5.3.14 Security measures for access control, including designated public access areas at Security Level 3

Define additional security measures to be taken at Security Level 3.

5.3.15 Security measures for restricted areas

The security plan shall define the restricted areas at the port facility. As a minimum, the restricted areas shall include the following.

— Shore areas immediately adjacent to each ship moored at the facility.

— Areas containing sensitive security information, including cargo documentation.

— Areas containing security and surveillance equipment and systems and their controls as well as lighting system controls.

— Areas containing critical facility infrastructure, including

- water supplies,
- telecommunications, and
- electrical systems.

— Access points for ventilation and air-conditioning systems.

— Manufacturing or processing areas and control rooms.

— Locations in the facility to which access by vehicles and personnel is restricted.

— Areas designated for loading, unloading, or storage of cargo and stores.

— Areas containing cargo consisting of dangerous goods.

5.3.16 Access to restricted areas

The security plan shall specify or define procedures to:

— determine which persons other than facility personnel are authorized to have access;

— determine the conditions under which that access may take place;

— define the extent of any restricted areas;

— define the times when access restrictions apply;

— control the entry, parking, loading, and unloading of vehicles;

— control the movement and storage of cargo and ship's stores;

— control unaccompanied baggage or personal effects;

— deter cargo tampering;

— prevent cargo that is not meant for carriage from being accepted and stored at the facility;

— identify cargo that is approved for loading onto ships interfacing with the facility;

— identify cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up;

— restrict the entry of cargo that does not have an appropriate, confirmed date for loading;

— ensure that cargo is released to the carrier specified in the cargo documentation;

— coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedures;

— create, update and maintain a continuous inventory, including locations of all dangerous goods or hazardous substances, from receipt to delivery within the facility;

— check cargo entering the facility for dangerous substances and devices at the rate specified in the approved PFSP; means for checking cargo include

  — visual examination,

  — physical examination, and

  — detection devices, such as scanners or canines;

— ensure routine checks of cargo, cargo transport units and cargo storage areas within the facility before and during cargo handling operations in order to deter tampering;

— ensure that cargo, containers, or other cargo transport units entering the facility match the delivery notes or equivalent cargo documentation;

— screen vehicles and personnel at the rate specified in the approved PFSP.

5.3.17 Security measures for handling cargo at Security Level 2

5.3.17.1 General

Define additional security measures to be taken at Security Level 2.

5.3.17.2 Security measures for handling cargo at Security Level 3

Define additional security measures to be taken at Security Level 3.

5.3.18 Security measures for delivery of ship's stores/spare parts and bunkers

5.3.18.1 Introduction

Define the security procedures relating to the delivery of ship's stores/spare parts as follows:

— check ship's stores for package integrity;

— prevent ship's stores from being accepted without inspection;

— deter tampering;

— screen ship's stores at the frequency specified in the approved PFSP;

— require advance notification of ship's stores or bunkers delivery, including a list of stores, delivery vehicle driver information, and vehicle registration information;

— screen delivery vehicles at the frequencies specified in the approved PFSP;

— escort delivery vehicles within the facility at the rate specified by the approved PFSP.

5.3.18.2 Security measures for delivery of ship's stores/spare parts and bunkers at Security Level 2

Define additional security measures to be taken at Security Level 2.

5.3.18.3 Security measures for delivery of ship's stores/spare parts and bunkers at Security Level 3

Define additional security measures to be taken at Security Level 3.

5.3.19 Security measures for monitoring

5.3.19.1 General

For the facility and its approaches on land and water, define the security measures that provide continuous monitoring through a combination of lighting, security guards, waterborne patrols and automatic intrusion-detection devices, or surveillance equipment, including the following:

— restricted areas within the facility;

— ships at the facility and areas surrounding the ships.

5.3.19.2 Security measures for monitoring at Security Level 2

Define additional security measures to be taken at Security Level 2.

5.3.19.3 Security measures for monitoring at Security Level 3

Define additional security measures to be taken at Security Level 3.

5.3.20 Security incident procedures

Define the procedures which ensure that the PFSO and facility security personnel are able to

— respond to security threats or breaches of security and maintain critical facility and ship-to-facility interface operations,

— evacuate the facility in case of security threats or breaches of security,

— report security incidents,

— brief all facility personnel on possible security threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects or activities, and

— secure non-critical operations in order to focus responses on critical operations.

5.3.21 Additional requirements for passenger and ferry port facilities

5.3.21.1 General

If the marine port facility receives passenger or ferry ships, the plan shall detail security measures to achieve the following.

— In a facility with no public access areas, establish separate areas for segregating unchecked persons and personal effects from checked persons and personal effects.

— Ensure that a defined percentage of vehicles to be loaded aboard are screened prior to loading, in accordance with the security level.

— Ensure that all unaccompanied vehicles to be loaded on passenger ships are screened prior to loading.

— Deny passengers access to restricted areas unless facility security personnel supervise them.

— In a facility with a designated public access area, provide sufficient security personnel to monitor all persons within the area and conduct screening of them and their personal effects, as needed.

5.3.21.2 Additional requirements for passenger and ferry port facilities at Security Level 2

Define the security measures to be taken to achieve the following in addition to the requirements for Security Level 1: Passenger or ferry facilities with no public access areas shall ensure screening of additional passengers, baggage, and vehicles prior to boarding the ship, as specified in the approved PFSP and Declaration of Security.

5.3.21.3 Additional requirements for passenger and ferry port facilities at Security Level 3

Define the security measures to be taken to achieve the following, in addition to the requirements for Security Level 2.

— Screen and identify all persons.

— Screen all baggage.

— Assign additional security personnel and patrols.

5.3.22 Additional requirements at cruise ship terminals

Define the security measures taken to achieve the following.

— Screen all persons, baggage, and personal effects for dangerous substances and devices.

— Check the identification of all persons seeking to board the ship. This includes confirming their reasons for boarding by examining joining instructions, passenger tickets, boarding passes, government identification or visitor badges, or work orders.

— Designate holding, waiting or embarkation areas to segregate screened persons and their personal effects from unscreened persons and their personal effects while they are awaiting embarkation.

— Provide additional security personnel to designated holding, waiting or embarkation areas.

— Deny passengers access to restricted areas unless facility security personnel supervise them.

5.3.23 Audits and security plan amendments

Define the port facility's policy for periodic review and audit of the PFSP. The PFSP shall be audited and revised as necessary when there is a change in the facility's ownership or operator, or if there have been modifications to the facility, including but not limited to physical structure, emergency response procedures, security measures or operations.

Auditing the PFSP as a result of modifications to the facility may be limited to those sections of the PFSP affected by the facility modifications.

5.3.24 Skills, knowledge and competencies of security and port facility personnel

5.3.24.1 General

Define the port facility's security training program, addressing how personnel are trained and evaluated to achieve the skills, knowledge and competencies as outlined in this subclause.

5.3.24.2 Skills, knowledge and competencies of port security officers (reference ISPS Part B 18.1)

The port security officer shall possess the following skills, knowledge and competencies.

— Security organization of the facility, including the size, chain of command, composition, type of equipment available, level of training and capability of the security force.

— General ship and facility operations and conditions. Know the facility throughout, including hours of operation; all cargo movement operations and cargo and shipping documents; composition and duties of the security workforce; facility restricted areas; public access areas (if any); and critical facility assets.

— Ship and facility security measures, including the meanings and the requirements of the different security levels. Know the procedures outlined in this security plan.

— Emergency preparedness, response and contingency planning.

— Security equipment and systems, including their operational limitations.

— Security equipment and systems and their uses on this facility. Be able to describe how they are affected by weather and power outages, and their resistance to deception. Be able to describe where the alarms sound and who is authorized to reset the alarms.

— Methods of conducting audits, inspections, control and monitoring techniques.

— Relevant international laws and codes and their recommendations.

— Relevant government legislation and regulations and their recommendations.

— Responsibilities and functions of local, provincial/state and national law enforcement agencies.

— Basic comprehension of risk assessment methodology.

— Methods of facility security surveys and inspections.

— Instruction techniques for security training and education, including security measures and procedures.

— Safeguarding sensitive security information and security-related communications.

— Current security threats and patterns.

— Recognizing and detecting dangerous substances and devices.

— Recognizing characteristics and behavioural patterns of persons who are likely to threaten security.

— Techniques used to circumvent security measures.

— Conducting physical searches and non-intrusive inspections.

— Conducting security drills and exercises, including exercises with ships.

— Assessing security drills and exercises.

5.3.24.3 Skills, knowledge and competencies of port facility personnel responsible for security duties (reference ISPS Part B 18.2)

Port facility personnel responsible for security duties shall possess the following skills, knowledge and competencies.

— Knowledge of current security threats and patterns.

— Recognition and detection of dangerous substances and devices.

— Recognition of characteristics and behavioural patterns of persons who are likely to threaten security.

— Techniques used to circumvent security measures.

— Crowd management and control techniques.

— Security-related communications.

— Knowledge of emergency procedures and contingency plans.

— Operation of security equipment and systems.

— Testing, calibration and maintenance of security equipment and systems.

— Inspection, control and monitoring techniques.

— Relevant provisions of the PFSP.

— Methods of physical screening of persons, personal effects, baggage, cargo and ship's stores.

— The meaning and the consequential requirements of the different security levels.

5.3.24.4 Skills, knowledge and competencies of all other facility personnel (reference ISPS Part B 18.3)

All other port facility personnel shall possess the following skills, knowledge and competencies.

— Relevant provisions of the PFSP.

— The meaning and the consequential requirements of the different security levels as they apply to them, including emergency procedures and contingency plans.

— Recognition and detection of dangerous substances and devices.

— Recognition of characteristics and behavioural patterns of persons who are likely to threaten security.

— Techniques used to circumvent security measures.

5.3.25 Drills and exercises

Define the policy and procedures which ensure that the PFSO conducts at least one security drill every 3 months and one exercise each calendar year, with no more than 18 months between exercises. Drills shall test individual elements of the PFSP, including response to security threats and incidents. Drills shall take into account the types of operations of the facility, facility personnel changes, the types of ships the facility is serving, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of law enforcement authorities. If a ship is moored at the facility on the date the facility has planned to conduct any drills, the facility may invite, but cannot require, the ship to participate in the facility's scheduled drill. Exercises test multiple elements of the PSFP. The PFSP shall define the drill and exercise program, including how the evaluation criterion will be developed.

5.4 Execution of the supply chain security plan

The organization shall establish a (or use existing) management system to enable its specific port facility security processes to be implemented.

6 Documentation

6.1 Safeguarding the documents

The documents developed to meet this document shall be safeguarded to prevent unauthorized disclosures. Define the plans that will be used to safeguard all the documents listed in this clause.

6.2 Port Facility Security Assessment Report

The Port Facility Security Assessment shall contain the following.

— A table of contents.

— Names and locations of the port facilities.

— Names and qualifications of persons performing security assessments.

— Dates the assessments were completed.

— Dates the assessments were revised.

— Dates the assessments must be redone.

— Letters of RSO authorization, if applicable.

— If more than one port facility is included, a letter from the IMO.

— Description/explanation of the port facility security assessment methodology used, including as a minimum a description of the threat scenarios considered, the methods used to classify consequences and likelihood, how risk was evaluated, and the methods used to determine where countermeasures were required.

— Detailed maps/charts of the areas that were assessed, with scales that identify the following (if they are within the area being assessed for the marine port facilities):

- accesses, entrances, approaches, anchorages and manoeuvring and berthing areas;
- cargo facilities, terminals, storage areas, and cargo handling equipment;
- systems such as electrical distribution, radio, and telecommunication systems;
- computer systems and networks;
- port/ship traffic-management systems and aids to navigation;
- power plants, cargo transfer piping, and water supplies;
- bridges, railways and roads;
- port service ships, including pilot boats, tugs, lighters, etc.;
- security and surveillance equipment and systems;
- waters adjacent to the port facility.

— A description of the current state of security in the port facility including the completed performance review list.

— A description of the nature of the port facility being assessed.

— A prioritized listing of risks to be addressed.

Included, should be a statement of limitations of the security assessment explaining that the security assessment conducted in accordance with this document is not designed to identify risks associated with a large internal conspiracy of ship or port facility personnel, truly random events, operational or security changes made after the assessment, changes to the vicinity outside the perimeter, persistent attacks on the port facility or the use of new or newly released technology. The security assessment is not a safety or health assessment, nor does it assess the proper operations of a port facility, other than the existing security procedures.

Also included, should be advice to the marine port facility operators, explaining that they shall ensure that the original assessment is revised to take into account any process or operation changes that occur, as well as changes in the port facility structures or the vicinities around the port facilities. A copy of this statement should be enclosed in each port facility's assessment report.

6.3 Marine Port Facility Security Plan

A current copy of the Marine PFSP shall be maintained for independent and authorized review.

6.4 Security operations and security training records

The following additional records shall be maintained.

— Training: for each security training session, the date of each session, duration of the session, a description of the training and a list of attendees.

— Drills and exercises: for each drill or exercise, the date held, description of drill or exercise, list of participants and any best practices or lessons learned that might improve the PFSP.

— Incidents and breaches of security: for each incident or breach of security, the date and time of occurrence, location within the facility, description of incident or breaches, to whom it was reported, and a description of the response.

— Changes in security levels: for each change in security level, the date and time of notification received and time of compliance with additional requirements.

— Maintenance, calibration and testing of security equipment: for each occurrence of maintenance, calibrations and testing, record the date and time and the specific security equipment involved.

— Security threats: for each security threat, the date and time of occurrence, how the threat was communicated, who received or identified the threat, description of threat, to whom it was reported and a description of the response.

— Declaration of Security (DoS): copy of each single-visit DoS and a copy of each continuing DoS for at least 90 days after the end of its effective period.

— Annual audit of the PFSP: for each annual audit, a letter certified by the PFSO stating the date the audit was completed.

6.5 Retention of records

All records pertaining to the marine port facility security assessment and security plan shall be maintained until a new assessment or security plan is completed. Unless otherwise specified in this document, all other records listed in this clause shall be maintained for at least 2 years.

Records required by this clause may be kept in an electronic format. If kept in an electronic format, they shall be protected against unauthorized deletion, destruction or amendment.

Annex A
(informative)

Guidance for obtaining advice and certification

A.1 General

Organizations intending to implement ISO 20858 are not obliged to obtain the services of an outside consultant. If an organization determines that it needs advice or help with carrying out security assessments, developing security plans or implementing the necessary requirements, it may seek external consulting services. It is, however, the responsibility of the organization seeking advice to check and verify the competence of consultants offering advisory services, for example by seeking recommendations, following up references or by reviewing work carried out. Consultants that provide services to the organization would be precluded from participating in third party audits of the same organization.

A.2 Demonstrating conformance with ISO 20858 by audit

ISO 20858 is a requirements standard intended to help organizations, which opt to voluntarily implement the requirements, establish and demonstrate their compliance with the International Maritime Organization, International Ships and Port Facility Security Code (ISPS) in a manner that can be verified by an outside auditor.

Types of audit:

— A first party audit is the self-determination of conformance by the organization itself.

— A second party audit is the determination or verification of an organization's conformance to agreed criteria by another organization, agency or body which has a vested interest in the organization's operations in the supply chain.

— A third party audit is a determination or verification of conformance to agreed criteria by an organization independent of all parties.

— Validation and certification by government or government agency.

A.3 Certification of ISO 20858 by third party certification bodies

If demonstration of compliance is sought through the third party audit process then the organization seeking certification should consider selecting a third party certification body accredited by a competent accreditation body, such as those which are members of the International Accreditation Forum Inc. (IAF) and subject to the IAF Multilateral Recognition Arrangement (MLA). Such accredited certification bodies comply with internationally recognised rules, codes of practice and audit protocols, such as ISO 17021 and ISO 19011. See section on notes.

Bibliography

[1] ISO 9001:2000, *Quality management systems — Requirements*

[2] ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*

[3] ISO 17021:2006, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

[4] ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*

[5] ISO 28000:2007, *Specification for security management systems for the supply chain*

[6] IAEA Publication INFCIRC/225/Rev. 4 (corrected), June 1999, *The Physical Protection Nuclear Material and Nuclear Facilities,* International Atomic Energy Agency, Vienna, Austria

[7] International Safety Management (ISM) Code, International Maritime Organization

[8] ISPS Code, amendment to the International Convention for the Safety of Life at Sea, International Maritime Organization (IMO), Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974, Agenda item 6 SOLAS/CONF.5/32 12 December 2002, *Consideration and adoption of amendments to the international convention for the safety of life at sea*, 1974, Parts A and B were in the same document and the Conference Resolution 9 was an attachment

[9] World Customs Organization, SAFE Framework of standards — Appendix to Annex 1

ICS 47.020.99

Price based on 30 pages