**Common requirements for security plan audits and reviews**

**12.** A maritime security plan for a port operator, port facility operator or port service provider must set out—

(a) a schedule of security plan audits by internal and external auditors;

(b) the circumstances, in addition to the occurrence of a maritime transport security incident, following which a security plan review must be conducted;

(c) the procedures for conducting a security plan audit, including a process for selecting auditors who are independent of the matters being audited; and

(d) the procedures for conducting a security plan review, including a process for consultation during the review.

**Port operator to give information**

**13.** A port operator required to have a maritime security plan must give to each port facility operator and port service provider conducting operations within the security regulated port—

(a) the information set out in item 17 (including contact details for the PSO);

(b) the measures to be used by the port operator to inform persons of the location of security zones established within the boundaries of the security regulated port; and

(c) the measures to confirm the identity of persons who are authorised to have access to security zones established within the boundaries of the security regulated port.

**Port facility operator to give information**

**14.** (1) A port facility operator required to have a maritime security plan must give the port operator of, and each port service provider conducting operations within, the security regulated port—

(a) the information set out in item 28 (including contact details for the PFSO);

(b) the measures to be used by the port facility operator to inform persons of the location of any security zones established within the boundaries of the port facility; and

(c) the measures to confirm the identity of persons who are authorised to have access to the port facility, to ships moored at the facility and to any security zones established within the boundaries of the port facility.

(2) A port facility operator required to have a maritime security plan must also give to the port operator details of the boundaries of the facility.

**Port service provider to give information**

**15.** A port service provider required to have a maritime security plan must give to the port operator of the security regulated port in which the provider conducts operations and to each port facility operator conducting operations within the security regulated port—

(a) the information set out in item 40 (including contact details for the PSPSO);

(b) the boundaries of the area under the control of the port service provider;

(c) details of the vessels operated by the provider (including the name, identification number, type, date, port of registry, and construction year of each vessel);

(d) the measures to be used by the port service provider to inform persons of the location of any security zones established within the boundaries of the land under the control of the port service provider; and

(e) the measures to confirm the identity of persons who are authorised to have access to the land under the control of the port service provider, to any security zones established within the boundaries of that land and to vessels operated by the provider.

***Division 2—Port operators***

*Subdivision 1—Matters to be dealt with in plan*

**General**

**16.** A maritime security plan for a port operator must cover all matters of ship/port interface—

(a) that are to be conducted within the security regulated port; and

(b) that are not covered by a maritime security plan for any other maritime industry participant that conducts operations within, or in connection with, the security regulated port.

**Port operator details**

**17.** A maritime security plan for a port operator must be accompanied by a document setting out the following information:

(a) name of the port operator;

(b) contact details for the port operator;

(c) name of the Chief Executive Officer of the port operator;

(d) name of the port for which the port operator has been designated;

(e) name of the port's harbour master;

(f) contact details for the harbour master;

(g) name or position of the person who is to be the PSO for the port;

(h) a single 24-hour fixed-line or mobile telephone number for the PSO.

**Security assessments**

**18.** In addition to the matters required by item 11, the security assessment that must be included in a maritime security plan for a port operator must include the following matters:

(a) a statement outlining the risk context or threat situation for the port;

(b) identification and evaluation of strategically important assets, infrastructure and operations that need to be protected;

(c) identification of possible risks or threats to assets, infrastructure and operations, and the likelihood and consequences of their occurrence;

(d) identification of existing security measures, procedures and operations;

(e) identification of gaps in port-wide security arrangements, including gaps arising from port infrastructure, human factors, policies and procedures;

(f) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

**Port security officer qualifications and responsibilities**

**19.** A maritime security plan for a port operator must set out—

(a) the knowledge, skills and other requirements for the PSO;

(b) the training or qualifications that satisfy the requirements mentioned in paragraph (a); and

(c) the training that must be given to the PSO.

**Other personnel with security role**

**20.** (1) A maritime security plan for a port operator must identify, by reference to their positions, port personnel with, or who have been assigned, security duties and responsibilities in addition to those of the PSO.

(2) The security duties and responsibilities of personnel so identified must be set out in the plan, together with—

(a) the knowledge, skills and other requirements for the security-related aspects of their positions;

(b) the training or qualifications that satisfy the requirements mentioned in paragraph (a); and

(c) the training that must be given to such personnel.

**Matters that must be in plan**

**21.** A maritime security plan for a port operator must address, in addition to the matters required by item 12, the following matters:

(a) measures to prevent unauthorised access to any security zones established in the security regulated port;

(b) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations in the port;

(c) procedures for responding to any security directions given by the Director-General;

(d) procedures for evacuation of the port in case of security threats or breaches of security;

(e) procedures for drills and exercises associated with the plan;

(f) procedures for interfacing with ship security activities;

(g) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to the port;

(h) procedures for reporting occurrences that threaten the security of the port;

(i) measures to ensure the security of the information contained in the plan;

(j) procedures in case the ship security alert system of a ship is activated while in the security regulated port;

(k) procedures for ensuring that the security of the port will be maintained in exceptional circumstances such as the presence of a ship in distress or of a ship seeking a place of refuge.

**Security of port in exceptional circumstances**

**21A.** A maritime security plan for a port operator must give sufficient guidance on how the security of the port will be maintained in exceptional circumstances such as the presence in the port of a ship in distress or of a ship that has been allowed to use the port as a place of refuge.

**Consultation and communication**

**22.** (1) A maritime security plan for a port operator must set out a mechanism for consultation—

(a) between the port operator and each of the maritime industry participants conducting operations within the security regulated port, for the purpose of coordinating their security-related activities; and

(b) between the port operator and its employees (or their representatives) regarding security measures and procedures to be implemented.

(2) A maritime security plan for a port operator must set out how the port operator will give notice in terms of regulations 23(2) and 27(2).

**Maritime security level 1**

**23.** A maritime security plan for a port operator must set out, in relation to maritime security level 1—

(a) the security measures, identified in the security assessment for the operation, for implementation at that level;

(b) the measures that have been implemented;

(c) a schedule for implementing the measures that have not been implemented; and

(d) any interim measures that will be implemented until the measures mentioned in paragraph (c) are fully implemented.

**Maritime security levels 2 and 3**

**24.** A maritime security plan for a port operator must set out, in relation to maritime security levels 2 and 3, the additional security measures that the operator will implement if the Director-General declares that maritime security level 2 of 3 is in force for the port.

**Declarations of security**

**25.** A maritime security plan for a port operator must provide for—

(a) the circumstances in which the operator will request a declaration of security with a ship;

(b) the procedures for negotiating the security measures and responsibilities of the operator and of the ship in those circumstances; and

(c) how security measures identified in a declaration will be implemented to ensure compliance by the operator and the ship with their security plans and with the declaration.

*Subdivision 2—Form of plan*

**Map of port**

**26.** The map that must accompany a maritime security plan for a port operator in terms of regulation 46(2) must—

(a) cover the whole security regulated port; and

(b) be of a size and scale that clearly shows the boundaries of the port and the location of any security zones established, or that the operator wishes to establish or change, within the area covered by the plan.

**Protection of plan**

**27.** A port operator must ensure that the maritime security plan for the operator is protected against unauthorised access, amendment and disclosure.

***Division 3—Port facility operators***

*Subdivision 1—Matters to be dealt with in plan*

**Port facility operator details**

**28.** A maritime security plan for a port facility operator must be accompanied by a document setting out the following information:

(a) name of the port facility operator;

(b) contact details for the port facility operator;

(c) name of the Chief Executive Officer of the port facility operator;

(d) name and location of the port facility;

(e) name of the port in which the facility is located;

(f) name or position of the person who is to be the PFSO for the facility;

(g) a single 24-hour fixed-line or mobile telephone number for the PFSO.

**Details of other maritime industry participants**

**29.** A maritime security plan for a port facility operator must be accompanied by a document setting out the name of, and contact details for—

(a) the PSO of the security regulated port in which the facility is located; and

(b) each port service provider conducting operations within the facility.

**Security assessments**

**30.** (1) In addition to the matters required by item 11, a security assessment for a port facility operator's operation must include the following matters:

(a) a statement outlining the risk context or threat situation for the port facility;

(b) identification and evaluation of important assets, infrastructure and operations that need to be protected;

(c) identification of possible risks or threats to assets, infrastructure and operations, and the likelihood and consequences of their occurrence;

(d) identification of existing security measures, procedures and operations;

(e) identification of weaknesses (including human factors) in the infrastructure, policies and procedures;

(f) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

(2) A security assessment for a port facility operator's operation must consider—

(a) the types of ships, and the types of cargoes transported by ships, served by the port facility; and

(b) any special risks or threats associated with such ships and cargoes.

**PFSO qualifications and responsibilities**

**31.** A maritime security plan for a port facility operator must set out—

(a) the knowledge, skills and other requirements for the PFSO;

(b) the training or qualifications that satisfy the requirements mentioned in paragraph (a); and

(c) the training that must be given to the PFSO.

**Other personnel with security role**

**32.** (1) A maritime security plan for a port facility operator must identify, by reference to their positions, port facility personnel with, or who have been assigned, security duties and responsibilities in addition to those of the PFSO.

(2) The security duties and responsibilities of personnel so identified must be set out in the plan, together with—

(a) the knowledge, skills and other requirements for the security-related aspects of their positions;

(b) the training or qualifications that satisfy the requirements mentioned in paragraph (a); and

(c) the training that must be given to such personnel.

**Matters that must be in plan**

**33.** A maritime security plan for a port facility operator must address, in addition to the matters required by item 12, the following matters:

(a) measures to prevent unauthorised carriage or possession of weapons or prohibited items in the facility or on board ships being loaded or unloaded at the facility;

(b) measures to prevent unauthorised access to the port facility, to ships moored at the facility and to any security zones established within the boundaries of the facility;

(c) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations in the port facility or ship/port interface;

(d) procedures for responding to any security directions given by the Director-General;

(e) procedures for evacuation of the port facility in case of security threats or breaches of security;

(f) procedures for drills and exercises associated with the plan;

(g) procedures for interfacing with ship security activities;

(h) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to the port facility;

(i) procedures for reporting occurrences that threaten the security of the port facility;

(j) measures to ensure the security of the information contained in the plan;

(k) measures to ensure security of cargo and of cargo handling equipment at the facility;

(l) procedures in case the ship security alert system of a ship is activated while in the security regulated port;

(m) procedures for facilitating—

(i) shore leave or relief of crew; and

(ii) access by visitors (including representatives of seafarer's welfare and of labour organisations).

**Consultation**

**34.** A maritime security plan for a port facility operator must set out, for the purpose of coordinating security-related activities, a mechanism for consultation—

(a) between the port facility operator and the port operator;

(b) between the port facility operator and each port service provider conducting operations within the security regulated port, and any other stakeholder, who may be affected by the implementation of the plan; and

(c) between the port facility operator and its employees (or their representatives) regarding security measures and procedures to be implemented.

**Maritime security level 1**

**35.** A maritime security plan for a port facility operator must set out, in relation to maritime security level 1—

(a) the security measures, identified in the security assessment for the operation, for implementation at that level;

(b) the measures that have been implemented;

(c) a schedule for implementing the measures that have not been implemented; and

(d) any interim measures that will be implemented until the measures mentioned in paragraph (c) are fully implemented.

**Maritime security levels 2 and 3**

**36.** A maritime security plan for a port facility operator must set out, in relation to maritime security levels 2 and 3, the additional security measures that the operator will implement if the Director-General declares that maritime security level 2 of 3 is in force for the port.

**Declarations of security**

**37.** A maritime security plan for a port facility operator must provide for—

(a) the circumstances in which the operator will request a declaration of security with a ship;

(b) the procedures for negotiating the security measures and responsibilities of the operator and of the ship in those circumstances; and

(c) how security measures identified in a declaration will be implemented to ensure compliance by the operator and the ship with their security plans and with the declaration.

*Subdivision 2—Form of plan*

**Map of port facility**

**38.** The map that must accompany a maritime security plan for a port facility operator in terms of regulation 46(2) must be of a size and scale that clearly shows—

(a) the boundaries of the port facility; and

(b) the location of any security zones established, or that the operator wishes to establish or change, within the area covered by the plan.

**Protection of plan**

**39.** A port facility operator must ensure that the maritime security plan for the operator is protected against unauthorised access, amendment and disclosure.

*Division 4—Port service providers*

*Subdivision 1— Matters to be dealt with in plan*

**Port service provider details**

**40.** A maritime security plan for a port service provider must be accompanied by a document setting out the following information:

(a) name of the port service provider;

(b) contact details for the port service provider;

(c) name of the Chief Executive Officer of the port service provider;

(d) name of each security regulated port in which the port service provider is located or operates;

(e) name or position of the person who is to be the PSPSO for the port service provider;

(f) a single 24-hour fixed-line or mobile telephone number for the PSPSO.

**Details of other maritime industry participants**

**41.** A maritime security plan for a port service provider must be accompanied by a document setting out the name of, and contact details for—

(a) each PSO of the security regulated port in which the port service provider is located or operates; and

(b) each port operator for, and port facility operator and port service provider conducting operations within, the security regulated port in which the port service provider is located or operates.

**Security assessments**

**42.** In addition to the matters required by item 11, a security assessment for the operation of a port service provider must include the following matters:

(a) a statement outlining the risk context or threat situation for the port service provider;

(b) identification and evaluation of important assets, infrastructure and operations that need to be protected;

(c) identification of possible risks or threats to assets, infrastructure and operations, and the likelihood and consequences of their occurrence;

(d) identification of existing security measures, procedures and operations;

(e) identification of weaknesses (including human factors) in the infrastructure, policies and procedures;

(f) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

**PSPSO qualifications and responsibilities**

**43.** A maritime security plan for a port service provider must set out—

(a) the knowledge, skills and other requirements for the PSPSO;

(b) the training or qualifications that satisfy the requirements mentioned in paragraph (a); and

(c) the training that must be given to the PSPSO.

**Other personnel with security role**

**44.** (1) A maritime security plan for a port service provider must identify, by reference to their positions, port service personnel with, or who have been assigned, security duties and responsibilities in addition to those of the PSPSO.

(2) The security duties and responsibilities of personnel so identified must be set out in the plan, together with—

(a) the knowledge, skills and other requirements for the security-related aspects of their positions;

(b) the training or qualifications that satisfy the requirements mentioned in paragraph (a); and

(c) the training that must be given to such personnel.

**Matters that must be in plan**

**45.** A maritime security plan for a port service provider must address, in addition to the matters required by item 12, the following matters:

(a) measures to prevent the introduction of unauthorised weapons or prohibited items into each security regulated port in which the port service provider is located or operates, or on board ships being served by the provider;

(b) measures to prevent unauthorised access to the land under the control of the port service provider, to any security zones established within the boundaries of that land and to vessels operated by the provider;

(c) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations of the port service provider;

(d) procedures for responding to any security directions given by the Director-General;

(e) procedures for evacuation in case of security threats or breaches of security;

(f) procedures for drills and exercises associated with the plan;

(g) procedures for interfacing with ship security activities;

(h) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to the port service provider;

(i) procedures for reporting occurrences that threaten the security of the port service provider;

(j) measures to ensure the security of the information contained in the plan;

(k) measures to ensure security of passengers, cargo and cargo handling equipment under the control of the port service provider;

(l) procedures in case the ship security alert system of a ship is activated while in the security regulated port.

**Consultation**

**46.** A maritime security plan for a port service provider must set out, for the purpose of coordinating security-related activities, a mechanism for consultation—

(a) between the provider and each port operator for the security regulated port in which the port service provider is located or operates;

(b) between the provider and each port facility operator and port service provider conducting operations within the security regulated port in which the port service provider is located or operates;

(c) between the provider and any other stakeholder who may be affected by the implementation of the plan; and

(d) between the provider and its employees (or their representatives), regarding security measures and procedures to be implemented.

**Maritime security level 1**

**47.** A maritime security plan for a port service provider must set out, in relation to maritime security level 1—

(a) the security measures, identified in the security assessment for the operation, for implementation at that level;

(b) the measures that have been implemented;

(c) a schedule for implementing the measures that have not been implemented; and

(d) any interim measures that will be implemented until the measures mentioned in paragraph (c) are fully implemented.

**Maritime security levels 2 and 3**

**48.** A maritime security plan for a port service provider must set out, in relation to maritime security levels 2 and 3—

(a) the security measures identified in the security assessment for the operation, for implementation at those levels; and

(b) the additional security measures that the provider will implement if the Director-General declares that maritime security level 2 or 3 is in force for the port.

**Declarations of security**

**49.** A maritime security plan for a port service provider must provide for—

(a) the circumstances in which the provider will request a declaration of security with a ship;

(b) the procedures for negotiating the security measures and responsibilities of the provider and of the ship in those circumstances; and

(c) how security measures identified in a declaration will be implemented to ensure compliance by the provider and the ship with their security plans and with the declaration.

*Subdivision 2—Form of plan*

**Map of port service provider**

**50.** The map that must accompany a maritime security plan for a port service provider in terms of regulation 46(2) must be of a size and scale that clearly shows—

(a) the boundaries of the area under the control of the port service provider; and

(b) the location of any security zones established, or that the provider wishes to establish or change, within the area covered by the plan.

**Protection of plan**

**51.** A port service provider must ensure that the maritime security plan for the provider is protected against unauthorised access, amendment and disclosure.

## PART 3—SHIP SECURITY PLANS AND ISSCs

***Division 1—Matters to be dealt with in ship security plan***

**Identification of ship**

**52.** A ship security plan must be accompanied by a document setting out the following information about the ship:

(a) name of the ship;

(b) the ship's official number;

(c) the ship's IMO ship identification number (if any);

(d) any other distinctive numbers or letters that identify the ship;

(e) type of ship;

(f) radio call sign;

(g) date and port of registry;

(h) year built;

(i) deadweight tonnage;

(j) gross registered tonnage;

(k) length and breath of ship;

(l) draft forward and aft (full load);

(m) number of crew;

(n) number of passenger berths;

(o) whether the ship is a foreign-going or coasting ship.

**Security assessments**

**53.** A ship security assessment for a South African regulated ship must include the following matters:

(a) the date when the assessment was completed or reviewed;

(b) the scope of the assessment, including assets, infrastructure and operations assessed;

(c) a summary of how the assessment was conducted, including details of the risk management process adopted;

(d) the skills and experience of the key persons who completed or participated in the assessment;

(e) the results of the examination and evaluation of the existing shipboard protective measures, procedures and operations;

(f) a statement outlining the risk context or threat situation for the ship, including consideration of trading routes;

(g) identification and evaluation of key shipboard operations that need to be protected;

(h) identification of possible risks or threats to the key shipboard operations and the likelihood and consequences of their occurrence;

(i) identification of existing security measures, procedures and operations;

(j) identification of weaknesses (including human factors) in the infrastructure, policies and procedures;

(k) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

**Ship operator, CSO and SSO**

**54.** (1) A ship security plan must be accompanied by a document setting out the following information:

(a) the name of the ship operator;

(b) the name of the Chief Executive Officer of the ship operator;

(c) the name or position of the person who is to be the CSO for the ship;

(d) a single 24-hour fixed-line or mobile telephone number for the CSO;

(e) the name or position of the person who is to be the SSO for the ship.

(2) A ship security plan may set out duties and responsibilities of a CSO or SSO that are in addition to the duties and responsibilities of a CSO and SSO in sections 11.2 and 12.2, respectively, of Part A of the ISPS Code.

(3) A ship security plan must set out how the CSO will communicate with the master of the ship if the Director-General or a maritime industry participant acting on behalf of the Director-General—

(a) gives notice that a maritime security level is in force for the ship; or

(b) gives a security direction to the ship.

**Shore-based personnel and crew with security role**

**55.** (1) A ship security plan must identify, by reference to their positions, shore-based personnel and crew with, or who have been assigned, security duties and responsibilities.

(2) The security duties and responsibilities of personnel and crew so identified must be set out in the plan, together with—

(a) the knowledge, skills and other requirements for the security-related aspects of their positions; and

(b) the training or qualifications that satisfy the requirements mentioned in paragraph (a).

**Training**

**56.** A ship security plan must set out the training that a CSO, SSO, and shore-based personnel and crew mentioned in item 55 must receive.

**Matters that must be in plan**

**57.** A ship security plan must address the following matters:

(a) measures to prevent unauthorised carriage or possession of weapons or prohibited items on board the ship;

(b) identification of on-board security zones;

(c) measures to prevent unauthorised access to the ship and any on-board security zones;

(d) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations of ship/port interface;

(e) procedures for responding to any security directions given by the Director-General or to directions given by a port state;

(f) procedures for evacuation of the ship in case of security threats or breaches of security;

(g) procedures for drills and exercises associated with the plan;

(h) procedures for interfacing with port, port service and port facility security activities;

(i) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to the ship;

(j) procedures for reporting occurrences that threaten the security of the ship;

(k) measures to ensure the security of the information contained in the plan.

**Maritime security level 1**

**58.** A ship security plan must set out, in relation to maritime security level 1—

(a) the security measures identified in the ship security assessment for implementation at that level;

(b) the measures that have been implemented;

(c) a schedule for implementing the measures that have not been implemented; and

(d) any interim measures that will be implemented until the measures mentioned in paragraph (c) are fully implemented.

**Maritime security levels 2 and 3**

**59.** A ship security plan must set out, in relation to maritime security levels 2 and 3—

(a) the security measures identified in the ship security assessment for implementation at those levels; and

(b) the additional security measures that the ship will implement if the Director-General declares that maritime security level 2 or 3 is in force for the ship.

**Declarations of security**

**60.** A ship security plan must provide for—

(a) the circumstances in which the ship will request a declaration of security with another ship or person;

(b) the procedures for negotiating the security measures and responsibilities of the ship and of the other ship or person in those circumstances; and

(c) how security measures identified in a declaration will be implemented to ensure compliance by the parties with their security plans and with the declaration.

**Security of ship in non-ISPS Code compliant ports**

**61.** (1) This item applies if it is envisaged by the ship operator that a South African regulated ship may call at ports or locations that are not port facilities or are port facilities the operators of which are not required to have, or do not have, security plans.

(2) A ship security plan must outline specific measures that will be implemented if the ship calls at ports or locations described in subitem (1) so that any risks associated with those ports or locations are not transferred to the ship.

**Security of ship in exceptional circumstances**

**62.** A ship security plan must give sufficient guidance on how the security of the ship will be maintained in exceptional circumstances such as search and rescue operations, humanitarian crises, extreme weather conditions and other emergencies.

**Pre-entry information**

**63.** (1) A ship security plan for a South African regulated ship that is a foreign-going ship must set out the procedures for giving pre-entry information in accordance with subitems (2) and (3).

(2) A South African regulated ship that is a foreign-going ship must be ready to give the following information (***pre-entry information***) not later than 48 hours before the ship enters South African waters in the course of a voyage:

(a) the security levels at which the ship operated at ports, and specific periods during which the ship operated at those levels, while conducting ship/port interface;

(b) any special or additional security measures that were implemented by the ship in any port where it conducted ship/port interface;

(c) whether appropriate ship security procedures were maintained during any ship to ship activity;

(d) if ship security procedures mentioned in paragraph (c) were maintained, the procedures and the specific periods during which those procedures were maintained.

(3) The information described in subitem (2) must be given in relation to the last 10 port calls by the ship.

**Maritime transport security incidents**

**64.** A ship security plan must set out procedures for—

(a) reporting maritime transport security incidents to the Authority; and

(b) responding to security threats and breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface.

**Security equipment**

**65.** A ship security plan must—

(a) include a list of the security equipment on board the ship;

(b) describe the measures to ensure the inspection, testing, calibration and maintenance of security equipment;

(c) set out the frequency for testing and calibration of security equipment; and

(d) set out procedures to ensure that only correctly calibrated security equipment is used on board the ship.

**On-board systems**

**66.** (1) A ship security plan must include information about the following systems on board the ship:

(a) external and internal communications systems;

(b) surveillance, identification, monitoring and reporting systems;

(c) tracking and positional systems.

(2) If a ship is provided with a ship security alert system, the ship security plan must—

(a) describe the operational characteristics of the system;

(b) describe the ship security alert that will be transmitted from the system;

(c) describe the performance standards to which the system must conform, being standards not inferior to those adopted by the International Maritime Organisation; and

(d) set out the procedures, instructions and guidance for using, testing, activating, de-activating and resetting the system, and for preventing false alarms.

**Ship security records**

**67.** A ship security plan must set out—

(a) the ship security records that are required to be kept on, by and for the ship in accordance with regulation 84;

(b) a plan for keeping and preserving ship security records; and

(c) the procedures for making those records available for inspection by a port state in accordance with regulation 84(3).

**Security plan audits and reviews**

**68.** A ship security plan must set out—

(a) a schedule of security plan audits by internal and external auditors;

(b) the circumstances, in addition to the occurrence of a maritime transport security incident, following which a security plan review must be conducted;

(c) the procedures for conducting a security plan audit, including a process for selecting auditors who are independent of the matters being audited; and

(d) the procedures for conducting a security plan review, including a process for consultation during the review.

***Division 2—Form of plan***

**Statement about authority of master**

**69.** A ship security plan must include a statement to the following effect:

"The master of the ship has the overriding authority and responsibility to make decisions with respect to the safety and security of the ship and to request the assistance of the ship operator or of any contracting government to the SOLAS Convention, as may be necessary.".

**Protection of plan**

**70.** The ship operator for a South African regulated ship must ensure that the ship security plan for the ship is protected against unauthorised access, amendment and disclosure.

**ANNEX 3**

(Regulation 120)

**FEES**

The following fees are payable to the Director-General:

| | | |
|---|---|---|
| | | |
| | | |
| | | |

# EXPLANATORY NOTE

*(This note is not part of the regulations)*

## THE DRAFT MERCHANT SHIPPING (MARITIME SECURITY) REGULATIONS, 2004

## OUTLINE

These Regulations are enabled by section 356 of the Merchant Shipping Act, 1951. Their purpose is to enhance maritime transport security by:

- establishing a maritime transport security regulatory framework, and providing for adequate flexibility within this framework to reflect a changing threat environment;
- implementing the mandatory requirements in Chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS), 1974, and the related International Ship and Port Facility Security (ISPS) Code, to ensure that South Africa remains in step with the international maritime transport security regime;
- ensuring that identified South African ports, and port facilities within them, operate with approved maritime security plans;
- ensuring that certain types of South African and other ships operate with approved ship security plans;
- issuing International Ship Security Certificates (ISSCs) to South African and certain other ships that have been security verified so that these ships will be able to enter ports in other SOLAS Contracting Countries; and
- establishing control mechanisms to impose control directions on foreign ships that are not compliant with the relevant maritime security requirements in these Regulations.

The Regulations have 10 parts:

**Part 1—Preliminary:** This Part includes the objects of the Regulations, their application and definitions. A detailed definition of the meaning of *unlawful interference with maritime transport* is included to clarify the application of the Regulations. Other detailed definitions include those of *security regulated ports*, *port operators* and *security regulated ships*. The Regulations will not apply to naval, military, customs, law enforcement, and other non-commercial government operated ships.

**Part 2—Maritime security levels and security directions:** This Part outlines the application of maritime security levels, security directions, and a system for notification. Maritime security level 1 will be the default level. Maritime security level 2 and maritime security level 3 will be declared by the Director-General when it is appropriate for a higher level of security to be put in place. In addition, in a security direction, which can be issued at security level 1, 2 or 3, the Director-General may direct maritime industry participants to comply with additional security measures when an unlawful interference with maritime transport is probable or imminent. The notification system ensures that those maritime industry participants and other persons who need to know about essential security level and security direction information are contacted.

**Part 3—Maritime security plans:** This Part requires certain maritime industry participants to have maritime security plans in force which must include security measures to be implemented at security levels 1, 2 and 3. Annex 2 of the Regulations provides additional detail on the content and form of these plans. The plans will be approved by the Director-General if adequate, may be cancelled by the Director-General in certain circumstances, and will be reviewed over time to maintain relevance.

**Part 4—Ship security plans and ISSCs:** This Part requires certain South African and other ships to have ship security plans in force which must include security measures and activities to be undertaken at security levels 1, 2 and 3. Annex 2 of the Regulations provides additional detail on the content and form of these plans. The plans will be approved by SAMSA if adequate, may be cancelled by SAMSA in certain circumstances, and will be reviewed over time to maintain relevance. Ships will be required to have ISSCs that will be issued upon ISSC verification. Division 5 of Part 4 sets out the requirements in relation to obtaining this certification.

**Part 5—Foreign regulated ships:** This Part requires certain foreign ships to provide pre-arrival information and their ISSCs to demonstrate their compliance with the Regulations. Foreign ships are also obliged to comply with the existing security levels. Ship operators of foreign regulated ships and masters of such ships are required to acknowledge communications regarding security levels and security directions. Part 5 includes compliance checking and control directions that foreign regulated ships may be subject to in the event of non-compliance with the Regulations.

**Part 6—Powers of officials:** This Part deals with authorised officers, who may exercise powers for the purpose of checking compliance with these Regulations and/or preventing unlawful interference with maritime transport.

**Part 7—Information-gathering:** This Part enables the Director-General to collect security compliance information from maritime industry participants. The collection of information is essential for the Director-General to deal with, and to resolve, compliance concerns before they become serious and compromise maritime security.

**Part 8—Enforcement orders:** This Part provides enforcement options in circumstances where contraventions of the Regulations have occurred or are suspected to have occurred. These enforcement options are:

- enforcement orders; and
- ship enforcement orders.

This Part gives the relevant regulator (i.e. the Director-General or SAMSA) the option to enforce compliance with the Regulations, instead of or in addition to referring matters to the prosecuting authorities. Prosecutions are resource intensive and while prosecution is an appropriate remedy for serious breaches of maritime security, the fundamental purpose of maritime security regulation is to encourage and effect compliance.

**Part 9—Miscellaneous**

This Part deals with security alert systems. It requires certain South African regulated ships to be fitted with a ship security alert system complying with SOLAS regulation XI-2/6.

**Part 10—Administrative arrangements and fees:** This Part deals with several administrative matters including alternative security agreements, exemptions, the exercise of the Director-General's powers and functions, and fees.

## NOTES ON REGULATIONS

### PART 1—PRELIMINARY

*Division 1—Title and commencement*

**Regulation 1 Title and commencement**

This regulation provides that the Regulations, once made, will be known as the *Merchant Shipping (Maritime Security) Regulations, 2004*.

It also provides that the Regulations commence in 2 stages:

1 the day the Regulations are published in the *Gazette*; and

2 1 July 2004.

The provisions commencing on publication in the *Gazette* are those that establish definitions, various processes (for example, the declaration of security regulated ports, the approval and cancellation of plans, the approval of training and equipment, ISSC verification and certification), and described the powers of authorised officers.

The provisions commencing on 1 July 2004 are, for example, those that create an obligation on maritime industry participants to comply with security plans, provide for some powers of officials and for the enforcement of provisions. This day is the day on which the Republic's obligations under the maritime security amendments to SOLAS enter into force.

The two stage commencement allows maritime industry participants time to familiarise themselves with their obligations and to have their plans prepared, approved and in place before the obligations and associated penalties come into force.

*Division 2—Purpose of regulations*

**Regulation 2 Purpose of regulations**

This regulation describes the purposes of the Regulations. The main purpose of the Regulations is to establish a regulatory framework that will safeguard maritime transport against unlawful interference. In particular, the framework is aimed at protecting ships, ports and port facilities within South Africa, and South African ships operating outside South Africa. The Regulations establish certain security requirements for maritime activities, requiring persons involved in these activities to meet certain obligations. For example, a particular obligation is the requirement of certain maritime industry participants to prepare and comply with security plans.

The implementation of this framework will enable South Africa to meet its obligations under the maritime security amendments to SOLAS.

*Division 3—Definitions*

**Regulation 3 Definitions**

This regulation defines certain terms used in the Regulations (these are in addition to the terms defined in section 2 of the Merchant Shipping Act, 1951). The definitions appear in

alphabetical order in the Regulations. The definitions are best read in conjunction with the relevant parts of the Regulations. A number of key definitions are included here.

*Declaration of security* means an agreement reached between a ship and other party (ship or a person) that identifies the security measures to be implemented by each party in specified circumstances.

*Foreign regulated ship* means a foreign ship that is:

- a passenger ship; or
- a cargo ship of 500 or more gross tonnes; or
- a mobile offshore drilling unit.

However, a ship is a foreign regulated ship only when it is in South African waters and is in, or proceeding to, a South African port.

*ISSC* means an International Ship Security Certificate, a document issued to a ship operator upon verification that the ship meets particular security requirements. Ship operators of regulated South African regulated ships will apply to the Authority for an ISSC. Ship operators of foreign regulated ships will need to present a valid ISSC issued for or on behalf of their flag state at any time while in South African waters and, in some cases, South African continental waters.

*Maritime industry participant* is defined to include persons who must have regard to maritime security matters as part of their business activities. A maritime industry participant includes:

- a port operator;
- a port facility operator;
- the ship operator for a South African regulated ship;
- the ship operator for a foreign regulated ship;
- a contractor who provides services to persons mentioned above;
- a port service provider.

*Maritime security levels* means the security levels, as advised by the Director-General, that will inform maritime industry participants which measures in their security plans need to be implemented at any given time. Maritime security level 1 will be in place unless the Director-General advises otherwise.

*Maritime security plan* is defined as a plan prepared for the purposes of Part 3. The plan includes a security assessment and details of measures to be implemented at each of the three maritime security levels. The maritime security plan is the key mechanism that maritime industry participants will use to guide their management of risks and implementation of security measures within their areas of responsibility.

*Port facility operator* means a person who operates a port facility, being an area within a security regulated port used wholly or partly for the loading or unloading of ships.

*Port operator* is defined as a person declared in Annex 1 to be the operator of a security regulated port.

*Port service provider* means:

- a lighter or barge operator;

- a line handling operator;
- a pilot boat operator;
- a tug operator;
- a person who provides certain offshore services, namely provisioning of ships, transhipment of goods or persons, and ship repair.

*Security officer* means a person designated by a maritime industry participant to implement and maintain:

- the participant's maritime security plan; or
- the ship security plan for a ship operated by the participant.

*Security regulated port* is defined as those areas of a South African port that are declared and described in Annex 1.

*Security regulated ship* includes South African regulated ships and foreign regulated ships that are subject to the security regulatory framework set out in these Regulations.

*Ship operator* means the owner of a security regulated ship, or a person who has an agreement with the owner of a security regulated ship to be the ship operator for the ship for the purposes of these Regulations, for example ship a management company or bareboat charterer.

*Ship security records* include:

- the ISSC for the ship;
- details of the ship's previous ten port calls and the security levelat which the ship operated at those calls; and
- certain parts of the ship security plan, consistent with the ISPS Code.

*South African continental waters* means:

- South African waters;
- the waters of South Africa's exclusive economic zone; and
- the waters beyond the outer limits of South Africa's exclusive economic zone but over South Africa's continental shelf.

*South African regulated ship* means:

- any of the following foreign-going ships having South African nationality:
    - passenger ships;
    - cargo ships of 500 or more gross tonnes;
    - mobile offshore drilling units (not on location); and
- mobile offshore drilling units in South African continental waters;
- fixed or floating platforms in South African continental waters.

*South African waters* means South Africa's internal and territorial waters.

*Division 4—Application*

**Regulation 4 Regulations not to apply to certain ships etc.**

This regulation provides that the Regulations do not apply to warships, naval auxiliaries and other ships owned or operated by the Government or a foreign state and used only on Government non-commercial service.

The Regulations also do not apply to ports and port facilities operated exclusively by the South African National Defence Force.

*Division 5—Unlawful interference with maritime transport*

**Regulation 5 Meaning of unlawful interference with maritime transport**

This regulation defines the term *unlawful interference with maritime transport*. The term is central to the application and understanding of the Regulations and their purpose. It defines the kinds of activities that constitute unlawful interference with maritime transport and therefore the kinds of activities that the Regulations are aimed at safeguarding against. It covers conduct that threatens the safe operation of ports and ships and that may cause harm to passengers, crew, port personnel and the general public or damage to property (whether on board or off a ship).

*Division 6—Security regulated ports and port operators*

**Regulation 6 Meaning of port**

This regulation defines the term *port* as an area of water, or land and water (including any buildings, installations or equipment situated in or on that land or water) intended for use either wholly or partly in connection with the movement, loading, unloading, maintenance or provisioning of ships.

To further clarify this meaning, a port may include:

- areas of water, located between the land of the port and the open waters outside the port, that are intended for use by ships to gain access to loading, unloading or other land-based port facilities; this includes, for example, the channels and approaches through which ships move from the open water to a berth;
- areas of open water intended for anchoring or otherwise holding ships before they enter areas of water described in paragraph (a);
- areas of open water between the areas of water described in paragraphs (a) and (b), for example an area such as a roadstead where a ship loads or unloads cargo or passengers brought from a land-based port facility by smaller vessels.

The definition has been used to comprehensively cover the meaning and intention of the term *port facility* as used in Chapter XI-2 of SOLAS. In Chapter XI-2 the definition of a port facility refers to a *location* where ship-port interfaces take place rather than an entity controlling, or having responsibility for, such interfaces. The definition refers to areas where direct ship-port interfaces take place as well as indirect interfaces, such as anchorages, waiting berths and seaward approaches.

**Regulation 7 Security regulated ports**

This regulation provides for the declaration of areas of a port to comprise a *security regulated port*. Security regulated ports are those areas of a port that are declared and described in Annex 1. These boundaries indicate where some of the key regulatory obligations for maritime industry participants under these Regulations begin and end.

A security regulated port will include the activities of a port operator, one or more port facility operators and other port service providers. For the purposes of these Regulations, a port facility does not have the same meaning as in Chapter XI-2 of SOLAS. In these Regulations, a port facility will be those areas at which direct and indirect ship-port interfaces take place, including, but not limited to, container terminals, bulk terminals, passenger terminals, common user facilities, and other port service providers falling within the meaning of a maritime industry participant and regulated under these Regulations.

**Regulation 8 Port operators**

This regulation provides the port operator for a security regulated port to be designated in Annex 1. The port operator should be able to demonstrate that it has responsibility for the relevant waterside and landside areas within a proposed or established security regulated port, for example control of vessel movement and management of port infrastructure.

The person designated as port operator will then be a maritime industry participant and responsible for ensuring that relevant obligations under these Regulations are met.

It is envisaged that the National Ports Authority (NPA) will be designated the port operator for all declared South African security regulated ports falling within NPA's jurisdiction.

***Division 7—Security regulated ships***

**Regulation 9 Meaning of security regulated ship**

This regulation defines the term *security regulated ship* and outlines the types of ships that are included in the regulatory framework established by these Regulations. Security regulated ships comprise South African regulated ships and foreign regulated ships.

**Regulation 10 Meaning of South African regulated ship**

This regulation defines a *South African regulated ship* as a ship falling into one of the following categories:

(a) South African foreign-going ships that are:

  (i) passenger ships; or

  (ii) cargo ships of 500 or more gross tonnage; or

  (iii) mobile offshore drilling units (not on location); or

(b) mobile offshore drilling units that are on location on or above South Africa's continental shelf;

(c) fixed or floating platforms that are situated on or above South Africa's continental shelf.

Government ships on commercial voyages are included if they fall into one of the categories outlined above.

Categories (b) and (c) include "ships" that are not otherwise subject to Chapter XI-2 of SOLAS. These "ships" are included to ensure broader coverage and better security for maritime operations over which South Africa has jurisdiction.

**Regulation 11 Meaning of foreign regulated ship**

This regulation defines *foreign regulated ship* to be foreign ships that fall into one or more of the following categories:

(a) passenger ships;

(b) cargo ships of 500 or more gross tonnage;

(c) mobile offshore drilling units,

and are in South African waters and in, or intending to enter, a South African port.

Foreign government ships on commercial voyages are included if they fall into one of the categories outlined above.

***Division 8—General defences***

This Division allows for a person to be excused from an offence when that person engages in conduct that would otherwise constitute an offence.

**Regulation 12 Ship master's decisions**

This regulation provides for the excuse to operate where it was necessary and reasonable for the master of a ship to take steps to protect the safety or security of the ship or its cargo, a person on or off the ship, another ship or a port, port facility or other installation within a port.

**Regulation 13 Complying with security directions**

This regulation provides for the excuse to operate where a person is required to do something in accordance with a security direction that would otherwise be an offence or a contravention of the Regulations or the Merchant Shipping Act, 1951. For example, a security direction may be given requiring a port operator to do something that conflicts with the measures set out in its maritime security plan. In such a case, if the port operator complies with the direction, he or she would not be taken to have committed the offence of not complying with the plan.

**Regulation 14 Complying with control directions**

This regulation provides for the excuse to operate where a person is required to do something in accordance with a security direction that would otherwise be an offence or a contravention of the Regulations or the Merchant Shipping Act, 1951. For example, a security direction may be given requiring a ship operator to do something that conflicts with the measures set out in a ship security plan for one of its ships. In such a case, if the ship operator complies with the direction, he or she would not be taken to have committed the offence of not complying with the plan.

*Division 9—Communicating with ship operators*

**Regulation 15 Communicating with ship operators**

This regulation provides that, where a person is required to give a notice or direction to a ship operator, the person may give that notice or direction to the shipping agent for the ship. This provision recognises the industry practice of communicating with ship operators and masters through the shipping agent.

**PART 2—MARITIME SECURITY LEVELS AND SECURITY DIRECTIONS**

A system of three maritime security levels will operate according to the prevailing threat environment, providing direction to maritime industry participants on the security measures that should be implemented. Maritime industry participants will be required in their security plans (plans are covered in Part 3 of the Regulations) to include information on the measures to be implemented at each level and must implement the measures according to the security level. The Director-General may, in certain circumstances, also give specific security directions on particular measures to be implemented.

*Division 1—Maritime security levels 1, 2 and 3*

**Regulation 16 Default security level (maritime security level 1)**

This regulation provides that the default security level is maritime security level 1. This means that, unless the Director General advises otherwise, maritime security level 1 applies at all times to each:

- security regulated port;
- South African regulated ship;
- area within a security regulated port; and
- maritime industry participant.

**Regulation 17 Director-General may declare maritime security level 2 or 3**

This regulation provides that, where there are grounds for raising the security level to 2 or 3, the Director-General will declare this in writing. A declaration may apply to one or more security regulated ports, South African regulated ships, areas within a security regulated port, maritime industry participants, or operations within or in connection with a security regulated port or ports.

The Director-General may also declare in writing that maritime security level 2 or 3 is in force for a foreign regulated ship. To clarify, this does not mean that, if a foreign regulated ship is operating at a higher security level than the port operator or port facility operator, any of these maritime industry participants will be obliged to match the foreign regulated ship's security level. A declaration of security will be required in such circumstances.

Subregulation (3) notes that the Director-General must only make a declaration of maritime security level 2 or 3 when a heightened risk to maritime transport has been identified and it is appropriate for increased security measures to be implemented for the port, ship, area (within a security regulated port), port facility or participant concerned.

**Regulation 18 Requirement for consultation**

This regulation requires the Director-General to consult the National Intelligence Coordinating Committee (Nicoc) before raising the security level to level 2 or 3.

**Regulation 19 When maritime security level in force**

This regulation provides that a security level declaration will remain in place for the port, ship, area or participant concerned until any period specified in the Director-General's declaration expires, or the Director-General revokes the declaration in writing.

**Regulation 20 Maritime security level declaration for port covers all port operations**

This regulation provides that, where the Director-General makes a declaration for a security regulated port, the declaration applies to each area or security regulated ship and any operations conducted by a maritime industry participant within the boundaries of the security regulated port.

**Regulation 21 Security levels and complying with plans**

This regulation provides that, where maritime security level 2 or 3 is in force, any affected maritime industry participant, area, port facility and operations of the participant, must comply with the corresponding measures set out in the security plan for that participant, area or operations. Regulation 41 makes it an offence for a maritime industry participant to fail to comply with their security plan.

Similarly, where the declaration affects a South African regulated ship, the corresponding measures set out in the ship security plan must be complied with. Regulation 59 makes it an offence for a ship operator to fail to comply with the security plan.

**Regulation 22 Maritime security level 1, 2 or 3 applies with security directions**

This regulation provides that, when a security direction is given, the entity to which the direction is given must comply with the requirements of that direction, but all other measures remain in place at the existing security level. For example, if maritime security level 2 is in force and a security direction is given, security level 2 measures remain in force and the specific security direction must also be complied with. Where any conflict occurs between the maritime security level 2 measures and the security direction, the security direction takes precedence.

***Division 2—Notifying maritime security level 2 and 3 declarations and revocations***

**Regulation 23 Notifying declarations covering security regulated ports**

This regulation describes the way in which the Director-General is required to communicate to affected port operators and maritime industry participants the fact that a maritime security level 2 or 3 declaration has been made.

The Director-General must notify the port operator and maritime industry participant with a maritime security plan in force of the declaration as soon as practicable. In turn, the port operator must, as soon as practicable, advise the following persons of the change in the security level:

- maritime industry participants covered by the port operator's plan, or who operate within the boundaries of the port (for example a tug operator or pilot); and
- the master of every security regulated ship within the port or about to enter the port. This will most likely occur when the security regulated ship confirms with the port operator that they are intending to enter a port.

Failure to pass on the level notification is an offence punishable by a fine (R20 000) or by imprisonment for a period not exceeding 12 months, or both. The offence does not apply if the port operator has a reasonable excuse.

Communicating the advice about the security level to be implemented will be critical to ensuring that all relevant maritime industry participants operating in the port and ships in or approaching the port have implemented measures commensurate with the security level, as outlined in each participant's security plan. The level of protection implemented by the measures will reflect the risks faced by each maritime industry participant as outlined in each participant's plan. If one or more participants are not notified of the change in security level, the port may be inadequately protected.

**Regulation 24 Notifying declarations covering security regulated ships**

This regulation provides that, when a declaration of a maritime security level is made for a security regulated ship, the Director-General must notify either the ship operator of the ship, who must pass it on to the master, or directly the master of the ship. The Director-General must also notify SAMSA and, if the ship is within a security regulated port, the port operator.

**Regulation 25 Notifying declarations covering areas within security regulated ports**

This regulation provides that declarations of a maritime security level made for an area within a security regulated port must be notified by the Director-General to maritime industry participants controlling those areas, and the port operator.

**Regulation 26 Notifying declarations covering maritime industry participants**

This regulation provides that declarations of a maritime security level made for maritime industry participants must be notified by the Director-General to both the participant concerned and the port operator of the port in which that participant conducts operations, if the participant is not the port operator.

**Regulation 27 Notifying revocations**

This regulation provides that, where the Director-General has advised a person that maritime security level 2 or 3 is in force and the declaration is revoked, he or she must, as soon as practicable, notify the person of the revocation.

Similarly, if a port operator has notified a person that security level 2 or 3 is in force, and the Director-General revokes the declaration, the port operator must as soon as practicable advise the person of the revocation. Failure to pass on the revocation notification is an offence punishable by a fine (R20 000) or by imprisonment for a period not exceeding 12 months, or both. The offence does not apply if the port operator has a reasonable excuse.

Adequate lines of communication, when a maritime security level is revoked, are important as maritime industry participants should not have to have security measures in place that are not commensurate with the risks faced at a particular time.

**Regulation 28 Communicating declarations and revocations**

This regulation provides that the Director-General may notify a security level declaration or revocation by facsimile or e-mail. It also allows a port operator to use the same communication methods as the Director-General.

***Division 3—Security directions***

**Regulation 29 Director-General may give security directions**

This regulation provides that the Director-General may direct that additional security measures be implemented or complied with. These directions are known as security directions and must be committed in writing before taking effect. The Director-General may issue security directions only if he or she reasonably believes that an unlawful interference with maritime transport is probable or imminent and that specific measures are appropriate to prevent the unlawful interference from occurring. Security directions are additional to the measures that maritime industry participants must comply with according to their approved plans.

**Regulation 30 Requirement for consultation**

This regulation requires the Director-General to consult Nicoc before giving a security direction. Subregulation (2) also requires that, where reasonable and practicable, the Director-General must consult certain people about a security direction that relates to the movement of a ship within, or in or out of, a security regulated port. Such a direction could have safety implications, for example it may not be possible for a ship to move safely at low tide or when it is partially loaded. By consulting with operational people at the port, such as maritime industry participants, the harbour master and the port security officer, the Director-General will be made aware of any safety implications of his or her directions.

The Director-General is also required to consult with organs of state whose operations may be affected by the control direction. This recognises that a number of such organs operate in ports, and many of them may have an interest in the movement of ships, for example SARS (customs and excise) must provide clearance before a ship can leave a South African port on an international voyage.

**Regulation 31 Confidentiality requirements**

This regulation provides that a security direction may include a requirement for confidentiality. This is intended to preserve the effectiveness of security measures that may be compromised if those intending to interfere with maritime security knew the details. Where a person is advised of the requirement for confidentiality, they have an obligation to protect the content of the security direction from unauthorised access or disclosure.

**Regulation 32 Persons to whom security directions may be given**

This regulation sets out the persons to whom security directions may be given. These may include maritime industry participants and their employees, passengers, and persons who are otherwise within the boundaries of a security regulated port. Where the Director-General issues security directions to passengers and persons other than maritime industry participants, the direction is given if it is clearly displayed at a place where the direction will be complied with.

A security direction given to a port operator may require the operator to communicate all or part of the direction to specified maritime industry participants who operate within the security regulated port. Failure to pass on the direction is an offence punishable by a fine (R20 000) or by imprisonment for a period not exceeding 12 months, or both. The offence does not apply if the port operator has a reasonable excuse.

**Regulation 33 Director-General may give security directions to security regulated ships**

This regulation provides that security directions may be given to security regulated ships, either to the ship operator of the ship, who must pass it on to the master, or directly to the master of the ship.

Failure by the ship operator to communicate the direction to the master of the ship is an offence punishable by a fine (R20 000) or by imprisonment for a period not exceeding 12 months, or both. The offence does not apply if the ship operator has a reasonable excuse.

**Regulation 34 When a security direction is in force**

In general, it is envisaged that because security directions are a threat response mechanism they will need to be in place as soon a practicable. In practice, it is recognised that the maritime transport industry may often require time to put the required measures in place. This regulation provides that a security direction comes into force at the time specified in the direction, although if no time is specified or the specified time is before the time when the direction is given, the direction comes into force 24 hours after it is given. Further, if the specified time is 7 days or more after the direction is given, the direction comes into force at the start of that day.

Security directions remain in force until the Director-General revokes them or the direction has been in force for 3 months. This requirement ensures that the security direction is current and appropriate to the circumstances. Any risk to maritime transport that requires increased security measures that go beyond 3 months duration will need to be addressed by changes to maritime security plans.

**Regulation 35 Revoking security directions**

This regulation provides that a security direction must be revoked if the unlawful interference, which was the subject of the direction, is no longer probable or imminent. The Director-General must notify the person to whom the direction was given of the revocation. Where a direction has been displayed, for example to passengers or other persons, the displayed direction must be removed.

**Regulation 36 Communicating security directions**

This regulation provides that the Director-General may give, communicate or revoke a security direction by facsimile or email, or orally.

The regulation allows a port or ship operator to use similar communication methods.

**Regulation 37 Offence (failing to comply with security directions)**

This regulation provides that it is an offence not to comply with a security direction that is in force and given to a person. The offence does not apply if the person has a reasonable excuse.

Penalty: fine (R20 000) or 12 months, or both.

**Regulation 38 Offence (failing to comply with confidentiality requirements)**

This regulation provides that it is an offence to fail to comply with a confidentiality requirement set out in a security direction. It is not an offence if the disclosure is to a court or to another body or person that has the power to require documents or answers to questions (eg. a court of marine enquiry).

Penalty: fine (R20 000) or 12 months, or both.

**PART 3—MARITIME SECURITY PLANS**

***Division 1—Maritime industry participants required to have maritime security plans***

**Regulation 39 Who must have security plans**

This regulation provides that the maritime industry participants who must have a maritime security plan in place are:

- port operators;
- port facility operators;
- port service providers that operate within the boundaries of a security regulated port; and
- port services providers that operate outside a security regulated port for the purpose of ship-port interface between a security regulated ship and a security regulated port.

However, a port service provider is not required to have a plan if the provider has agreed to its activities being covered by another maritime industry participant's plan and its activities are in fact so covered.

Division 6 of Part 1 deals with the identification of port operators of security regulated ports. Port facility operators required to have maritime security plans are those port facility operators located within security regulated ports.

**Regulation 40 Offence (operating without maritime security plan)**

This regulation makes it an offence for a maritime industry participant to operate without a maritime security plan in force when one is required, unless the participant has a reasonable excuse.

Penalty: fine (R20 000) or 12 months, or both.

**Regulation 41 Offence (failing to comply with maritime security plan)**

The purpose of a maritime security plan will be to detail the measures that the maritime industry participant will implement at any given security level. In order to protect against unlawful interference with maritime transport, the participant must ensure that the measures are fully implemented as set out in the plan. Failure to comply with a maritime security plan could potentially result in an opportunity for unlawful interference to occur.

Therefore, this regulation makes it an offence for a maritime industry participant to fail to comply with a plan that is in force for the participant, unless the participant has a reasonable excuse.

Penalty: fine (R20 000) or 12 months, or both.

***Division 2—Complying with other plans***

**Regulation 42 Complying with maritime security plans of other participants**

This regulation provides that maritime industry participants must not hinder or obstruct compliance with the maritime security plan of another maritime industry participant. For example, a maritime industry participant (who is not required to have an approved security plan) must take all reasonable steps to comply with a port facility operator's approved security procedures when operating at the port facility's premises.

Maritime industry participants with security plans in force must not only be given the relevant parts of another maritime industry participant's security plan with which they are required to comply, they are required to agree, in writing, to their activities being covered by another maritime industry participant's security plan. This is intended to create a record of each party's knowledge of the arrangement and their obligations under it.

Where a maritime industry participant does obstruct compliance with another participant's plan, the participant does not commit an offence but may be subject to an enforcement order. The objective of this provision is that the participant ceases the conduct that is obstructing compliance.

**Regulation 43 South African regulated ships must not hinder or obstruct compliance with maritime security plans**

This regulation provides that the operations of a South African regulated ship must not interfere with or obstruct compliance with a maritime security plan. Where the operations do obstruct compliance, either or both of the ship's operator or master may be subject to an enforcement order.

Obligations on foreign regulated ships are dealt with in Division 1 of Part 5.

*Division 3—Content and form of maritime security plans*

**Regulation 44 Content of maritime security plans**

This regulation provides that a key component of the maritime security plan is the security assessment of the participant's operation. The purpose of the security assessment is to ensure that a risk-based systematic and analytical process is conducted on the likelihood and consequences of a potential unlawful interference with maritime transport.

The security plan, which is to be developed on the basis of the security assessment, will set out the security measures to be implemented at maritime security levels 1, 2 and 3. These measures will be informed by the security assessment and will address the individual circumstances and operational requirements of maritime industry participants.

The plan must demonstrate that implementation will contribute towards reducing the risk of unlawful interference with maritime transport. In particular, a security plan must provide the contact details of the participant's security officer and make provision for the use of declarations of security. A declaration of security may be required for specific situations, such as a ship calling at a port when the ship is operating at a higher level of security than the port.

Security assessments must take into account the obligations set out in the ISPS Code. Moreover, the Director-General may require maritime industry participants to take into account certain documents in completing their security assessments, for example, threat and security environment information. Annex 2 of the Regulations requires other matters to be addressed by the security assessment, for example the basic elements of security assessments and the key matters to be covered in security assessment submissions.

The Director-General will issue guidance material to assist maritime industry participants in the preparation of maritime security plans that should be taken into account when the plan is prepared.

**Regulation 45 Additional requirements for maritime security plans**

This regulation provides that Annex 2 of the Regulations prescribes specific matters that are to be dealt with in, and addressed in relation to, maritime security plans, whether in all plans, plans for a particular kind of maritime industry participant, or plans for a particular class of a particular kind of maritime industry participant. For example, different security requirements may be determined for operators of bulk liquid facilities and for container terminals.

**Regulation 46 Form of maritime security plan**

This regulation provides that maritime security plans must be in writing and prepared according to the requirements set out in Annex 2. It also requires a maritime security plan to be accompanied by a map, which must be prepared in accordance with the requirements set out in Annex 2.

*Division 4—Approving, revising and cancelling maritime security plans*

**Regulation 47 Providing maritime security plans for approval**

This regulation states that a maritime industry participant wishing to operate with a maritime security plan may submit the plan to the Director-General for approval. This

provision reflects the procedure to be adopted by a maritime industry participant that operates within a declared security regulated port and is required to have a security plan in force.

**Regulation 48 Approving maritime security plans**

This regulation provides that the Director-General will approve a plan in writing if he or she is satisfied that the plan addresses the relevant requirements under Division 3. If the Director-General is not satisfied, he or she must refuse to approve the plan and advise the participant in writing of the refusal and give reasons for the refusal.

The Director-General is taken to have refused to approve the plan if a participant has given the Director-General a plan and the Director-General does not provide any written notice of approval, or refusal to approve, within 90 days after the plan was submitted. The participant may seek a review of a decision or deemed decision to refuse to approve a plan.

**Regulation 49 When maritime security plan in force**

This regulation provides that the plan comes into force (i.e. the operator implements the plan and compliance may be enforced) at a time specified in the notice of approval. If the time specified in the notice is earlier than the time at which the notice is given, or the notice does not specify a time, the plan is deemed to come into force when the notice is given.

The plan remains in force until it is replaced or the approval of the plan is cancelled.

**Regulation 50 Director-General may direct variations of maritime security plans**

This regulation reflects that, in changing circumstances, the Director-General is able to direct a participant to carry out specific variations to a plan. The Director-General may, by written notice, give a direction to vary where he or she is no longer satisfied that the plan is adequate for the purposes of Division 3. The directed variation should address the requirements under Division 3. The notice must detail what the required variation is, and the timeframe within which the participant must give the Director-General the varied plan. If the participant does not give the Director-General the varied plan within the specified period, or within any further allowed period, the Director-General must cancel the approval of the plan.

**Regulation 51 Participants may revise maritime security plans**

This regulation provides that maritime industry participants may also provide revised plans to the Director-General for approval on their own initiative. Where the participant wishes to revise the plan, the approval process as described in regulations 48 and 49 applies. The revised plan, once approved, replaces any other plan for the participant in force at that time.

**Regulation 52 Director-General may direct participants to revise maritime security plans**

This regulation provides that the Director-General may direct the participant in writing to revise the plan (and submit the revised plan for approval) where he or she believes that the plan no longer adequately addresses the relevant requirements under Division 3. The

direction to revise the plan must include a specified time period within which the participant must give the Director-General the revised plan. If the participant does not give the Director-General the revised plan within the specified time period, or within any further period allowed by the Director-General, the Director-General must cancel the approval of the plan in writing. This provision reflects the need to have security plans remain current and responsive to the security environment during the life of the plan.

**Regulation 53 Maritime security plans must be revised every 5 years**

This regulation requires that plans must be revised every five years, unless the Director-General has approved a revised plan for the participant within that period. If the maritime industry participant does not submit a revised plan for approval (in accordance with the established approval procedures) when the existing plan has been in force for 5 years, the approval of the existing plan is automatically cancelled.

**Regulation 54 Cancelling inadequate maritime security plans**

This regulation provides that a plan may be cancelled if the Director-General believes that the plan no longer adequately addresses the requirements under Division 3 and that it would not be appropriate to direct either a variation or a revision of a plan. The Director-General must cancel the approval of the plan in writing.

**Regulation 55 Cancelling for failure to comply with maritime security plans**

This regulation provides that the Director-General may cancel the approval of a plan if the maritime industry participant has failed to comply with the plan.

It is envisaged that this power will be used only in those cases where a lesser measure, such as an enforcement order to rectify the non-compliance, is not complied with.

**Regulation 56 Cancelling maritime security plans on request**

This regulation provides that a maritime industry participant may request the Director-General in writing to cancel the approval of the participant's plan, for example where a participant of a particular kind ceases to operate as a participant of that kind or where the activities of the participant are to be covered by another participant's maritime security plan.

PART 4—SHIP SECURITY PLANS AND ISSCs *etc*

This Part deals with the requirement for South African regulated ships to have ship security plans, International Ship Security Certificates (ISSCs), and certain ship security records. The responsibilities of foreign regulated ships are dealt with in Part 5.

*Division 1—Ships required to have ship security plans*

**Regulation 57 Which ships must have ship security plans**

This regulation provides that South African regulated ships must have ship security plans in place. South African regulated ships are defined in Division 7 of Part 1.

**Regulation 58 Offence (operating without a ship security plan)**

This regulation makes it an offence for a ship operator to operate a South African regulated ship without a ship security plan in force, unless the operator has a reasonable excuse.

Penalty: fine (R20 000) or 12 months, or both.

**Regulation 59 Offence (failing to comply with ship security plan)**

This regulation makes it an offence for a ship operator to operate a South African regulated ship not in accordance with the plan, unless the operator has a reasonable excuse.

Penalty: fine (R20 000) or 12 months, or both.

***Division 2—Complying with other plans***

**Regulation 60 Complying with ship security plans of other ships**

This regulation is intended to prevent the operations of a South African regulated ship from interfering with the compliance of a ship security plan of another ship. Where such obstruction does occur, an enforcement order may be sought against the ship operator for, or the master of, the ship causing the obstruction.

**Regulation 61 Maritime industry participants must not hinder or obstruct compliance with ship security plans**

This regulation is intended to prevent the operations of a maritime industry participant from interfering with the compliance of a ship security plan. Where such obstruction does occur, the participant may be subject to an enforcement order.

***Division 3—Content and form of ship security plans***

**Regulation 62 Content of ship security plans**

This regulation provides that a ship security plan must include a security assessment. The purpose of the security assessment is to ensure that a risk-based systematic and analytical process is conducted on the likelihood and consequences of a potential unlawful interference with maritime transport.

The security plan will set out the security activities or measures to be undertaken or implemented at maritime security levels 1, 2 and 3. These activities or measures will be informed by the security assessment and will address the individual circumstances and operational requirements of the ship. The plan must demonstrate that implementation will contribute towards reducing the risk of unlawful interference with maritime transport.

In particular, a security plan must provide the contact details of the ship's security officer and make provision for the use of declarations of security. A declaration of security may be required for specific situations such as a ship visiting a port that is not a security regulated port or the ship calling at a port when the ship is operating at a higher level of security than the port.

SAMSA may require certain documents to be taken into account in completing security assessments, for example, threat and security environment information. Annex 2 of the Regulations requires other matters to be addressed in the security assessment, for example, the basic elements of security assessments and the key matters to be covered in security assessment submissions.

SAMSA will issue guidance material to assist in the preparation of ship security plans that should be taken into account when the plan is prepared.

**Regulation 63 Additional requirements for ship security plans**

This regulation provides that Annex 2 of the Regulations prescribes specific matters that are to be dealt with in, and addressed in relation to, ship security plans, whether in all plans, plans for operators of a particular kind of ship, or plans for operators of a particular class of a particular kind of ship. For example, different security requirements may be determined for operators of bulk liquid ships and for container ships.

**Regulation 64 Form of ship security plans**

This regulation provides that ship security plans must be in writing and prepared in accordance with the requirements set out in Annex 2 of the Regulations.

***Division 4—Approving, revising and cancelling ship security plans***

**Regulation 65 Providing ship security plans for approval**

This regulation reflects the process that operators of South African regulated ships wishing to operate their ships will need to prepare a ship security plan and submit it to SAMSA for approval.

**Regulation 66 Approving ship security plans**

This regulation provides that SAMSA will approve a plan in writing if it is satisfied that the plan addresses the relevant requirements under Division 3. If SAMSA is not satisfied, it must refuse to approve the plan and advise the participant in writing of the refusal and outline reasons for the refusal.

SAMSA is taken to have refused to approve the plan if the ship operator has given SAMSA a plan and SAMSA does not provide any written notice of approval, or refusal to approve, within 90 days after the plan was submitted.

**Regulation 67 When ship security plan in force**

This regulation provides that once the plan has been approved, it comes into force (ie it is operational and compliance may be enforced) at the time specified in the approval notice. Where the approval notice does not specify a time, or the time specified is earlier than the time the notice was given, the plan is deemed to come into force when the notice is given.

The plan remains in force until it is replaced or the approval of the plan is cancelled.

**Regulation 68 Authority may direct variations of ship security plans**

This regulation reflects the potential for changing circumstances and the need for SAMSA to be able to direct specific variations to a plan. SAMSA may, by written notice, direct the operator of the ship to vary the plan if SAMSA is no longer satisfied that the plan adequately addresses the requirements set out in Division 3. The notice must set out the required variation and specify the period within which the operator must provide the new plan. If the operator does not provide a new plan in accordance with the notice and within the timeframe specified, or any further time allowed by SAMSA, SAMSA must cancel the approval of the plan.

**Regulation 69 Ship operator may revise ship security plan**

This regulation provides that ship operators may also provide revised plans to SAMSA for approval on their own initiative. Where the operator wishes to revise the plan, the approval process as described in regulations 66 and 67 applies. The revised plan, once approved, replaces any other plan for the ship in force at that time.

**Regulation 70 Authority may direct ship operator to revise ship security plan**

This regulation provides that SAMSA may, by written notice, direct the operator of a South African regulated ship to revise the ship security plan if SAMSA believes that the plan is no longer adequate with regard to the requirements set out in Division 3. Where the operator does not provide a revised plan within the specified period, or within any further period allowed by SAMSA, SAMSA must cancel the approval of the plan.

**Regulation 71 Ship security plans must be revised every 5 years**

This regulation requires that ship security plans must be revised every five years, unless SAMSA has approved a revised plan for the participant within that period. If the ship operator does not submit a revised plan for approval (in accordance with the established approval procedures) when the existing plan has been in force for 5 years, the approval of the existing plan is automatically cancelled.

**Regulation 72 Cancelling inadequate ship security plans**

This regulation provides that a ship security plan may be cancelled if SAMSA believes that the plan no longer adequately addresses the requirements under Division 3 and that it would not be appropriate to direct either a variation or a revision of a plan.

**Regulation 73 Cancelling for failure to comply with ship security plan**

This regulation provides that SAMSA may cancel the approval of a ship security plan if the ship operator has failed to comply with the plan.

It is envisaged that this power will be used only in those cases where a lesser measure, such as an enforcement order to rectify the non-compliance, is not complied with.

**Regulation 74 Cancelling ship security plans on request**

This regulation provides that a ship operator may request SAMSA in writing to cancel the approval of the ship security plan.

*Division 5—International Ship Security Certificates*

**Regulation 75 Which ships must have ISSCs**

This regulation provides that South African regulated ships must have an International Ship Security Certificate (ISSC).

For South African regulated ships, the possession of an ISSC will verify that the ship has implemented its approved security plan.

**Regulation 76 Offence (operating without an ISSC)**

This regulation makes it an offence for the ship operator of a South African regulated ship to operate the ship without an ISSC or interim ISSC in force, unless there is a reasonable excuse.

Penalty: fine (R20 000) or 12 months, or both.

**Regulation 77 Applying for ISSC**

This regulation provides that the process to obtain an ISSC is for the operator of a South African regulated ship to apply in accordance with the requirements determined in writing by SAMSA.

**Regulation 78 Conditions for giving ISSC**

This regulation provides that SAMSA must issue an ISSC to the ship operator of a South African regulated ship if the applicant has a ship security plan in force (which has been approved in accordance with the provisions under Division 4), and the ship has been ISSC verified.

**Regulation 79 ISSC verification**

ISSC verification forms part of the process for issuing the ISSC. This regulation provides that following application for the ISSC, the ship will be ISSC verified by an authorised officer in accordance with procedures determined in writing by SAMSA. The verification will signify that the ship meets the requirements determined in writing by SAMSA, and an ISSC will be issued. Generally speaking, the authorised officer will inspect the ship to verify that the ship is operating in accordance with the procedures set out in its approved ship security plan.

Subregulation (3) provides that if an ISSC is in force and an authorised officer finds that the ship does not meet SAMSA's requirements for ISSC verification, the ship is no longer ISSC verified. The officer may allow a period of time for the ship to rectify compliance with the requirements for verification.

**Regulation 80 When ISSC in force**

This regulation provides that an ISSC comes into force when it is issued and will remain in force until:

- cancelled by the Authority; or
- the ship operator is no longer the operator of that ship; or

- five years expire after the ISSC was issued.

**Regulation 81 Cancelling ISSCs**

This regulation provides that SAMSA must cancel an ISSC if the ship no longer has a security plan in force (i.e. if the security plan has been cancelled), or the ship no longer meets the requirements for ISSC verification.

**Regulation 82 Interim ISSCs**

This regulation provides that an interim ISSC may be issued by SAMSA if the ship operator has applied for an ISSC, has a security plan in place but has not yet been ISSC verified, and SAMSA believes that the ship would be ISSC verified if it were to be inspected.

To facilitate the transfer of ships from one operator to another, interim ISSCs may be issued to a ship operator who has become the operator of a South African regulated ship that had an ISSC before the transfer of operations.

Interim ISSCs remain in force for a period specified in the interim ISSC but not exceeding 6 months.

**Regulation 83 Offence (false or misleading statements in relation to having ISSC)**

This regulation makes it an offence for the master of a South African regulated ship to engage in conduct that suggests that an ISSC or interim ISSC is in force for the ship when this is not the case. The offence also applies if the false or misleading conduct is made to another SOLAS Contracting Government.

Penalty: fine (R20 000) or 12 months imprisonment, or both.

***Division 6—Ship security records***

**Regulation 84 Ship security records**

This regulation requires that a South African regulated ship keep certain information. This list is based on SOLAS regulation XI-2/9.2. The information may be requested by a foreign port state to confirm compliance by the ship with the requirements of the ISPS Code.

This regulation requires that the information must be kept on board the ship for 7 years. The information may be considered in any audit or review, and may be used by an authorised officer.

**PART 5—FOREIGN REGULATED SHIPS**

***Division 1—Obligations on foreign regulated ships***

**Regulation 85 Foreign regulated ships must have ISSCs**

This regulation requires that the ship operator for a foreign regulated ship must have a valid International Ship Security Certificate (ISSC) or an approved ISSC equivalent for the ship. The ship must also carry the required ship security records.

A valid ISSC will be issued to a foreign ship by or on behalf of its flag state in accordance with that state's acceptance of the ISPS Code. ISSCs may be issued by another flag state or a recognised security organisation (such as classification societies), where for example a foreign state has delegated this function to an RSO or a flag state is not a signatory to SOLAS.

SAMSA may approve in writing a certification to be an approved ISSC equivalent. The provision will facilitate the entry into South African security regulated ports of ships that meet ISPS Code security standards but have not been issued with an ISSC.

The master of a foreign regulated ship must be able to show the ISSC or ISSC equivalent and other ship security records to South African authorities. This is likely to occur during port inspections but may also occur at any time while the ship is in South African territorial waters.

If the ship operator fails to have the required ship security records on board, the master or the ship operator may be given a control direction by SAMSA.

**Regulation 86 Foreign regulated ships must provide pre-arrival information**

This regulation compels masters of foreign regulated ships to provide certain security information prior to their arrival in South African waters or entry into a port, as part of pre-arrival reporting procedures.

The Director-General will prescribe the requirements for the provision of pre-arrival information including the information to be provided, to whom, when, the circumstances, and the form and manner in which this information is to be given. The Director-General may determine that different pre-arrival information is to be provided before entering different places or areas within South Africa.

If the master fails to comply with this provision, SAMSA may give a control direction to the master or the ship operator.

**Regulation 87 Foreign regulated ships must allow inspections *etc***

This regulation provides that the master of a foreign regulated ship must allow an authorised officer to board the ship for inspection in accordance with the powers of an authorised officer set out in Part 6. For clarity this regulation provides that the master must provide the ship security records to an officer when requested to do so. If the master does not allow an officer to inspect the ship, then the master, or the ship operator, may be given a control direction by SAMSA.

**Regulation 88 Foreign regulated ships must comply with security levels**

This regulation sets out a number of security measures that foreign regulated ships must comply with when in South African waters. The ship must be at security level 1 unless otherwise declared by the Director-General. If the Director-General declares that security level 2 applies to a security regulated port a foreign ship in that port must implement ISPS level 2 measures. ISPS level 2 measures are measures that should, under the ISPS Code, be implemented when maritime security level 2 is in force. The ship specific measures to be implemented by the ship at ISPS level 2 will be contained in the ship's security plan, as approved by its flag state. Similar requirements apply if the Director-General declares that security level 3 applies to a port.

The provision also acknowledges that a ship may have been directed by its flag state to implement a higher security level than would otherwise apply under this regulation. In these circumstances, the ship must comply with the directions received from its flag state.

If a foreign regulated ship does not implement security measures appropriate to the security level declared by the Director-General, the ship operator for the ship or the ship's master may be given a control direction by SAMSA.

**Regulation 89 Meaning of ISPS level 1, 2 and 3 measures**

This regulation defines that ISPS level 1, 2 and 3 measures applicable at security levels 1, 2 and 3 respectively are those that should be implemented as provided in the ISPS Code. The types of measures to be implemented are described in general terms in the ISPS Code. Foreign regulated ships with ISSCs will have details of specific security measures to be implemented at these security levels in their individual ship security plans.

**Regulation 90 Foreign regulated ships must comply with security directions**

This regulation provides that if the Director-General gives a security direction to a foreign regulated ship the ship must comply with this direction. If the ship does not comply, the ship operator or master may be given a control direction by SAMSA.

In addition to the control direction, the master of the ship and the ship operator may incur a penalty for failing to comply with a security direction under regulation 33, unless the operator has a reasonable excuse.

**Regulation 91 Complying with maritime and ship security plans**

This regulation provides that a foreign regulated ship must not operate so as to compromise compliance with a maritime security plan of a maritime industry participant or a ship security plan of a South African regulated ship. If the operations do compromise compliance, the ship operator or the master of the foreign regulated ship may be given a control direction by SAMSA.

**Regulation 92 Acknowledging level notifications and directions**

This regulation provides that if the master of a foreign regulated ship has received notice that maritime security level 2 or 3 is in place for the ship or a control direction has been given to the ship, and the master does not acknowledge receipt of such notice or direction, the master commits an offence.

Similar offences may also apply to the operator of the foreign regulated ship.

Penalty: fine (R20 000) or 12 months imprisonment, or both.

***Division 2—Control directions***

**Regulation 93 Authority may give control directions**

This regulation provides the major regulatory powers over foreign regulated ships. Under this regulation SAMSA may give control directions to the ship operator or master of a foreign regulated ship to either control the movement of the ship or require the master or operator to take specific action or refrain from specific action. SAMSA may only give a control direction if it is required to ensure compliance with the obligation imposed on

foreign regulated ships under these regulations or in respect of a special measure to enhance maritime security as set out in SOLAS Chapter XI-2. For example, if a master fails to provide a valid ISSC for a ship the ship may be denied entry into a South African port.

Control directions include, but are not limited to:

- removing the ship from South African waters;
- removing the ship from a security regulated port;
- moving the ship to another location within the port;
- holding the ship in a certain position for a specified period or until a specified event occurs;
- taking particular actions on board the ship;
- allowing an authorised officer on board the ship to inspect the ship or the ship security records carried by the ship.

**Regulation 94 Requirement for consultation**

This regulation requires that, where reasonable and practicable, SAMSA must consult with certain people about control directions. SAMSA has broad powers to order the movement of regulated foreign ships under regulation 93. Such an order could have safety implications, for example it may not be possible for a ship to move safely at low tide or when it is partially loaded. By consulting with operational people at the port, such as maritime industry participants, the harbour master and the port security officer, SAMSA will be made aware of any safety implications of its directions.

SAMSA is also required to consult with organs of state whose operations may be affected by the control direction. This recognises that a number of such organs operate in ports, and many of them have an interests in the movement of ships, for example SARS (customs and excise) must provide clearance before a ship can leave a South African port on an international voyage.

**Regulation 95 Communicating control directions**

This regulation allows SAMSA to communicate a control direction by facsimile or e-mail, or orally.

**Regulation 96 Offence (failing to comply with control direction)**

This regulation makes it an offence for the master of, or ship operator for, a foreign regulated ship to fail to comply with a control direction, unless there is a reasonable excuse.

Penalty: fine (R20 000) or 12 months imprisonment, or both.

**PART 6—POWERS OF OFFICIALS**

This Part deals with the powers, functions and responsibilities of certain officials under these Regulations in preventing unlawful interference with maritime transport. It sets out who are authorised officers, their powers and the limits on their powers. The primary role of authorised officers is to conduct ISSC verifications and to audit and investigate the

compliance of maritime industry participants with the Regulations. In order to do this effectively, they require a number of powers, including the power to enter premises and ships and inspect documents.

**Regulation 97 Authorised officers**

This regulation sets out the categories of persons who are authorised officers for the purposes of the Regulations.

**Regulation 98 Authorised officers' powers (ISSC verifications)**

This regulation provides that an authorised officer may inspect a South African regulated ship for ISSC verification including the inspection of ship security records and other security related documents on board the ship. The purpose of the inspection is to determine whether the ship has implemented security measures in order to meet the requirements for ISSC verification. Regulation 79 sets out those requirements.

**Regulation 99 Authorised officers' powers (ships)**

This regulation provides an authorised officer with a number of powers he or she may exercise in determining whether a person or ship is complying with the Regulations and, if non-compliance is suspected, to investigate a possible contravention. These powers are essential to the ability of the Director-General and SAMSA to monitor and investigate compliance with the Regulations and fulfil their role as regulator. This regulation gives authorised officers the ability to board and inspect any part of a security regulated ship, inspect and photograph equipment, observe and record operating procedures (including training drills), discuss operating procedures with crew or other maritime industry participants (eg port service providers) and inspect and copy a range of security related documents.

**Regulation 100 When powers may be exercised (ships)**

This regulation limits when an authorised officer may exercise his or her powers on board a ship. An authorised officer may exercise his or her powers at any time and without notice if the ship is within the boundaries of a security regulated port. However, if the power is to be exercised outside those boundaries, reasonable notice must be given to the ship operator or the master of the ship.

**Regulation 101 Authorised officers' powers (participants)**

This regulation provides an authorised officer with a number of powers he or she may exercise in determining whether a person or ship is complying with the Regulations and if non-compliance is suspected to investigate a possible contravention. These powers are essential to the ability of the Director-General and SAMSA to monitor and investigate compliance with the Regulations and fulfil their role as regulator. This regulation gives an authorised officer the ability to enter and inspect any area, building, vehicle or vessel under the control of a maritime industry participant. If a maritime industry participant operates from a residence the officer's powers of entry are limited to that part of the residence that are used for those operations. The officer may also inspect and photograph equipment, observe operating procedures (including training drills), discuss operating procedures with employees or other maritime industry participants (eg port service

providers), inspect and copy documents and operate equipment in order to access a document or record kept by a maritime industry participant.

**Regulation 102 When powers may be exercised (participants)**

This regulation provides that an authorised officer may exercise his or her powers within the boundaries of a security regulated port at any time and without notice. However, if the power is to be exercised outside those boundaries, reasonable notice must be given to the maritime industry participant.

PART 7—INFORMATION GATHERING

This Part allows the Director-General to obtain security compliance information from maritime industry participants. The collection of security compliance information is important for ensuring that appropriate security measures are implemented and maintained to safeguard against unlawful interference with maritime transport, and that South Africa has met its international obligations.

**Regulation 103 Director-General may require security compliance information**

This regulation enables the Director-General to require information from maritime industry participants that can be used to assess participants' compliance, or non compliance, with their maritime security plans, ship security plans, or other security-related obligations under these Regulations. Such information is security compliance information. If the Director-General has reasonable grounds to believe that the participant has security compliance information he or she may require the information from a participant. The information must be given within the period and in the form and manner specified in the Director-General's written notice. The time period in which information must be given must not be less than 14 days. The Director-General may specify that the participant provide the information orally, in writing, and/or by electronic transmission.

Failure to comply with the Director-general's notice is an offence unless the participant has a reasonable excuse.

Penalty: fine (R20 000) or 12 months imprisonment, or both.

This regulation will allow the Director-General to assess the health of the security of the maritime industry and will enable the Director-General to recognise possible weaknesses in the maritime security system and rectify problems before the safety of the industry and the public is compromised.

**Regulation 104 Self-incrimination**

Subregulation (1) clarifies that whenever a person is required to give security compliance information that person cannot be excused from giving the information on the grounds that it might incriminate them or expose them to a penalty.

In acknowledgment that coercive information-gathering powers, where the common law privilege is removed, must be accompanied by appropriate protection for the informant, subregulation (2) provides that the individual giving the information and any information, document or thing obtained directly or indirectly as a result of giving information cannot be admitted as evidence in a criminal proceeding, or any other proceeding for the recovery of a penalty, against the person. This protection does not extend to the giving of false or misleading information or documents as provided under regulation 105. This

regulation reinforces the concept that the processes of gathering compliance information to improve maritime security and those relating to judicial proceedings, particularly criminal proceedings, should be separate to ensure a continued free flow of security compliance information. Giving security compliance information should be encouraged so that issues regarding compliance can be addressed before they compromise maritime transport security or put the general public in danger.

**Regulation 105 Offence (false or misleading information)**

This regulation makes it an offence to given false or misleading security compliance information.

Penalty: fine (R20 000) or 12 months, or both.

**PART 8—ENFORCEMENT ORDERS**

An enforcement order is a regulatory instrument that may be issued when the Director-General or SAMSA is of the opinion that a breach of the Regulations has occurred and that specific action is required (or stopped or restricted) in order to safeguard against unlawful interference with maritime transport. Use of an order reflects the policy that rectification of a problem is the preferred outcome to prosecution.

***Division 1—Enforcement orders for maritime industry participants***

**Regulation 106 Director-General may make enforcement orders**

This regulation allows the Director-General to make enforcement orders prohibiting or restricting specified activities or requiring specific action by a maritime industry participant named in the enforcement order. The Director-General's power to issue an enforcement order must be based on a reasonable belief that the maritime industry participant has contravened a provision in these Regulations and that the order is necessary to safeguard against unlawful interference with maritime transport.

**Regulation 107 Commencement and duration of enforcement orders**

This regulation provides that an enforcement order comes into force at the time specified in the order, for example 1:00 am on a particular day, or if there is no specified time, at the beginning of the 7th day after the order is made. The provision for a shorter period will allow for orders to be given in emergency situations. An enforcement order remains in force either for the period specified in the order, or if a period is not specified, until the Director-General revokes the order.

**Regulation 108 Reviewing enforcement orders**

To ensure enforcement orders remain current and relevant, this regulation provides for their regular review. Under this regulation the Director-General must review enforcement orders at least every 3 months, and after each review, confirm, vary or revoke the order in writing. This reflects the fact that enforcement orders are aimed at rectification of a particular problem and should be monitored to ensure the activities or actions specified in the order continue to address that particular contravention.

An order must be revoked unless the Director-General is satisfied that the order is still required to safeguard against unlawful interference with maritime transport.

The Director-General must not vary the order unless he or she is satisfied that the order as varied adequately safeguards against unlawful interference with maritime transport and the varied order bears a dear and direct relationship to the contravention and remains proportionate to the contravention.

Subregulation (4) clarifies that an order continues in force as varied, and will require a further review after an additional 3 months.

**Regulation 109 Notifying enforcement orders**

This regulation provides that the Director-General must, as soon as is practicable after making or reviewing an enforcement order, inform the maritime industry participant named in the order of the making or review of the order.

Subregulation (2) provides that failure by the Director-General to comply with subregulation (1) does not affect the validity of an order.

**Regulation 110 Offence (failing to comply with enforcement order)**

This regulation makes it an offence for a maritime industry participant to fail to comply with an enforcement order, unless the participant has a reasonable excuse.

Penalty: fine (R20 000) or 12 months, or both.

***Division 2—Ship enforcement orders for South African regulated ships***

This Division details provisions for the issuing of enforcement orders to the ship operator or master of a South African regulated ship. The provisions are similar to the enforcement orders able to be issued to other maritime industry participants in that the conditions which must be satisfied and the circumstances under which an order may be issued are the same but an order is limited to the taking or stopping of specified action in relation to the ship.

**Regulation 111 Ship enforcement orders (South African regulated ships)**

This regulation allows SAMSA to issue a ship enforcement order to the ship operator for a South African regulated ship or the master of the ship requiring the ship operator or the master to take specified action, or refraining from specified action, in relation to the ship.

SAMSA's power to issue a ship enforcement order is limited to those instances where SAMSA reasonably believes that the ship has contravened a provision in these Regulations and it is necessary to make the order to safeguard against unlawful interference with maritime transport.

A ship enforcement order must bear a clear and direct relationship to the contravention and be proportionate to the contravention. Some of the actions that may be required include removing the ship from specified waters or port, or moving or holding the ship within a port.

These orders are similar to the control directions SAMSA may give to foreign regulated ships in certain circumstances under Division 2 of Part 5.

**Regulation 112 Requirement for consultation**

This regulation requires that, where reasonable and practicable, SAMSA must consult with certain people about ship enforcement orders. SAMSA has broad powers to order the movement of South African regulated ships under regulation 111. Such an order could have safety implications, for example it may not be possible for a ship to move safely at low tide or when it is partially loaded. By consulting with operational people at the port, such as maritime industry participants, the harbour master and the port security officer, SAMSA will be made aware of any safety implications of its directions.

SAMSA is also required to consult with organs of state whose operations may be affected by the control direction. This recognises that a number of such organs operate in ports, and many of them have an interests in the movement of ships, for example SARS (customs and excise) must provide clearance before a ship can leave a South African port on an international voyage.

**Regulation 113 Communicating ship enforcement orders**

This regulation allows SAMSA to communicate a ship enforcement order by facsimile or e-mail, or orally.

**Regulation 114 Offence (failing to comply with ship enforcement order)**

This regulation makes it an offence for a ship operator or master to fail to comply with a ship enforcement order, unless there is a reasonable excuse.

Penalty: fine (R20 000) or 12 months, or both.

**PART 9—MISCELLANEOUS**

**Regulation 115 Ship security alert system**

This regulation provides that certain types of South African regulated ships must have a ship security alert system. It also specifies the timeframe in which the ship security alert system must be fitted.

The regulation also provides certain functional requirements of a ship security alert system. These requirements are based on SOLAS regulation XI-2/6.

**PART 10—ADMINISTRATIVE ARRANGEMENTS AND FEES**

**Regulation 116 Alternative security agreements**

This regulation recognised the possibility that the Government may enter into an alternative security agreement under the terms of SOLAS. The regulation provides that the Director-General is to supervise the alternative arrangements and to periodically review the operation of the agreement.

The regulation also recognises the possibility of an agreement of this kind varying or replacing these Regulations in relation to the matters covered by the agreement.

**Regulation 117 Exemptions**

This regulation allows the Minister to grant exemptions from the requirements of these regulations. An exemption may not be inconsistent with the obligations set out in SOLAS Chapter XI-2 and the ISPS Code.

**Regulation 118 Powers and functions of Director-General**

This regulation provides that the Director-General may authorise a senior management service employee in the Department of Transport to exercise some or all of the Director-Generals powers and functions under these Regulations.

This regulation recognises that the Director-General is unlikely to be able to exercise all his or her powers and functions personally all the time.

**Regulation 119 Director-General may establish co-ordinating structures**

This regulation provides that the Director-General may establish structures to facilitate efficient administration of these Regulations.

This regulation recognises the need to co-ordinate the activities of the different roleplayers in the security field.

**Regulation 120 Fees (Director-General's functions)**

This regulation and Annex 3 establish the fees to be paid for functions performed by the Director-General.

SAMSA has power to impose charges under the South African Maritime Safety Authority Act, 1998.

## ANNEX 1—SECURITY REGULATED PORTS

This Annex must be read in conjunction with regulations 7 and 8. It describes the areas in South African ports that constitute security regulated ports for the purposes of these Regulations. It also designates the person who is to be the port operator for a described port.

## ANNEX 2—SECURITY PLANS

### PART 1—PRELIMINARY

**Item 1 Definitions**

This item defines many terms used in the Annex.

**Item 2 Port security officers**

This item requires that the port operator designate a port security officer (PSO) before submitting the port security plan to the Director-General.

Subitem (2) allows the PSO to be designated by name or by reference to a position. Designation by position is more flexible when the person occupying the position changes.

Subitem (3) lists the duties and responsibilities of the PSO. These duties are based on the requirements of section 17.2 of Part A of the ISPS Code and on the role of the port in coordinating security across the security regulated port.

Subitem (4) requires that the port operator ensure that the PSO is able to perform the listed duties.

**Item 3 Port facility security officers**

This item requires that the port facility operator designate a port facility security officer (PFSO) before submitting the port facility security plan to the Director-General for approval.

Subitem (2) allows the port facility security officer to be designated by name or by reference to a position. Designation by position is more flexible when the person occupying the position changes.

Subitem (3) requires that the port facility security officer perform certain duties, including those listed in section 17.2 of Part A of the ISPS Code.

Subitem (4) requires that the port facility operator ensure that the PFSO is able to perform the listed duties.

**Item 4 Port service provider security officers**

This item requires that the port service provider designate a port service provider security officer (PSPSO) before submitting the port service provider security plan to the Director-General for approval.

Subitem (2) allows the PSPSO to be designated by name or by reference to a position. Designation by position is more flexible when the person occupying the position changes.

Subitem (3) lists the duties and responsibilities of PSPSO. These duties are based on the requirements of section 17.2 of Part A of the ISPS Code.

Subitem (4) requires that the port service provider ensure that the PSPSO is able to perform the listed duties.

**Item 5 Company security officers**

This item requires that a ship operator designate a company security officer (CSO) before the ship security plan is submitted to SAMSA for approval.

Subitem (2) allows the CSO to be designated by name or by reference to a position. Designation by position is more flexible when the person occupying the position changes.

Subitem (3) requires that the CSO perform certain duties, including the duties required in section 11.2 of Part A of the ISPS Code.

Subitem (4) requires that the ship operator ensure that the CSO is able to perform the listed duties.

**Item 6 Ship security officers**

This item requires that the ship operator designate a ship security officer (SSO) for each ship. The SSO may be designated by name or by position. Designation by position may be more flexible on ships where the personnel changes are frequent.

Subitem (3) requires that the SSO perform certain duties, including those listed in section 12.2 of Part A of the ISPS Code.

Subitem (4) requires that the ship operator ensure that the SSO is able to perform the listed duties.

Subitem (5) requires that if the SSO is not the master of the ship, that the SSO is accountable to the master. This requirement preserves the master's overriding accountability for the safety and security of the ship as stated in section 6.1 of Part A of the ISPS Code and also in item 69 of this Annex.

**Item 7 Delegation by security officers**

This item allows security officers to delegate some or all of their powers (except the power of delegation) to another person who is able to perform the delegated duties. This power of delegation is necessary because it will be difficult for one person to perform all the duties of a security officer, particularly being contactable 24 hours a day. The delegation may also be used when the security officer will be absent from work.

**Item 8 Shore-based personnel and crew**

This item requires that the ship operator identify personnel and crew other than the security officers, who have security responsibilities, and ensure that those people are able to perform their security duties.

**Item 9 Declarations of security**

This item requires that a declaration of security be signed by people responsible for security on behalf of the parties to the declaration. The item also ensures that certain security information is included in the declaration, and that the declaration is retained for future audit and security planning processes.

**Item 10 Security plan audits and reviews**

This item requires that maritime and ship security plans are audited and reviewed in accordance with the requirements of the approved maritime or ship security plan. Failure to do this will be a failure to comply with the maritime or ship security plan, and may be an offence under regulation 41 or 59.

Subitem (2) requires that a review is also conducted after a maritime transport security incident. This will ensure that the relevant maritime industry participant consider the adequacy of the security measures in the plan in light of an incident.

Subitem (3) requires that records of an audit or review be kept for 7 years. These records may be considered in a future audit or review, and may be used by an authorised officer.

## PART 2—MARITIME SECURITY PLANS

*Division 1—Preliminary*

### Item 11 Common requirements for security assessments

This item provides that all security assessments must include information about when, how and by whom the security assessment was completed or reviewed and what is covered by the security assessment.

### Item 12 Common requirements for security plan audits and reviews

This item provides that a maritime security plan for a port operator, port facility operator or port service provider must include information about when a security plan will be audited and reviewed, and the procedures for conducting audits and reviews. It is important that maritime security plans are subject to ongoing independent audit and review to ensure that they remain adequate and relevant.

### Items 13, 14 and 15 Port operator, Port facility operator and Port service provider to give information

These items provide that a port operator, port facility operator and port service provider must share certain information with other maritime industry participants within the port. It is important that maritime industry participants who are required to have security plans have access to certain information about each others' maritime security plans to ensure effective implementation of security measures and procedures. Other relevant security information may be shared through the consultation processes required in items 22, 34 and 46.

*Division 2—Port operators*

*Subdivision 1—Matters to be dealt with in the plan*

### Item 16 General

This item requires that the maritime security plan for a port operator must cover all ship/port interfaces within the security regulated port that are not covered by another maritime security plan. In practice, this means that the port operator will be responsible for matters of ship/port interface occurring on the water-side, and for any areas of land within the security regulated port that are not controlled by a port facility operator or a port service provider. The boundaries of the security regulated port are described in Annex 1.

### Item 17 Port operator details

This item requires that the maritime security plan be accompanied by certain information that identifies the port operator who owns the plan and their contact details. The information required in this item may change more frequently than the security arrangements in the plan and needs to be updated quickly and easily. The information is not part of the plan because the process required in Part 3 Division 4 for the Director-General to approve changes to maritime security plans is not required for this

information. The information is not about the security measures to be implemented and does not require approval by the Director-General.

**Item 18 Security assessments**

This item requires that security assessments address several key matters. These requirements are consistent with the ISPS Code and general risk assessment. The matters also reflect the port operator's role in the identification of port-wide gaps in security that require treatment.

**Item 19 Port security officer qualifications and responsibilities**

This item requires that a port operator ensure that each person employed as a port security officer or delegate of a port security officer meet certain knowledge and skill requirements as established by the port operator. It also requires that a port operator's plan provide suitable training to the port security officer. The Director-General will consider the proposed knowledge and training when deciding whether to approve the plan. Records of training undertaken may be subject to audit by an authorised officer.

**Item 20 Other personnel with security role**

This item requires that the port operator consider the security responsibilities of employees other than the port security officer and ensure that they have appropriate knowledge and receive training. The Director-General will consider the proposed knowledge and training when deciding whether to approve the plan and the records of this training may be subject to audit by an authorised officer.

**Item 21 Matters that must be in plan**

This item requires that the port operator address certain matters in their security plan. These matters are analogous to the requirements of the ISPS Code for port facility operators. The measures and procedures for these matters should include those identified in the security assessment.

**Item 22 Consultation and communication**

This item requires that a port operator consult with the other maritime industry participants within the port and with employees. This will ensure that security measures implemented by the various maritime industry participants in a port complement each other, and promote a strong security culture within the port.

Subitem (2) also requires that a port operator's plan include how they will fulfil their obligations to pass on information about security directions and changes of security level. This information may need to be conveyed quickly and it is important that there be a clearly understood mechanism for communication of security directions across the port.

**Item 23 Maritime security level 1**

This item requires that the maritime security plan detail the measures to be implemented that are appropriate to the ordinary operating environment of the port. The measures and procedures will vary depending on the types and levels of risks identified in the security assessment.

Paragraph (d) also recognises that not all measures in the plan will be implemented immediately. For example, there may be some delay for items requiring major capital investment. In this situation, the maritime security plan should provide that interim measures are in place until the permanent measures can be fully implemented. The Director-General will consider the schedule for implementation and the appropriateness of the interim measures when making the decision to approve a maritime security plan.

**Item 24 Maritime security levels 2 and 3**

This item requires that the maritime security plan includes additional security measures that can be implemented during times of heightened risk to maritime transport. This reflects the requirement of the ISPS Code for three security levels. The Director-General has the power to change the security level in regulation 17.

**Item 25 Declarations of security**

This item requires that the maritime security plan provide for declarations of security (DOS). The ISPS Code provides for DOS as a way for ports and ships to ensure that security is maintained during a ship/port interface. A ship may agree to a DOS with a port operator, or with more than one maritime industry participant within the port, for example a port facility operator and one or more port service providers may also be party to a DOS.

*Subdivision 2—Form of plan*

**Item 26 Map of port**

This item requires that a port operator provide a map or maps that meet the requirements in regulation 46(2) and (3).

**Item 27 Protection of plan**

This item requires that the port operator must protect the maritime security plan from unauthorised access, amendment or disclosure. The value of the preventive security measures and procedures in maritime security plans may be compromised if the plans are disclosed to persons without authority to view or possess them.

***Division 3—Port facility operators***

*Subdivision 1—Matters to be dealt with in plan*

**Item 28 Port facility operator details**

This item requires that the maritime security plan be accompanied by certain information that identifies the port operator who owns the plan and their contact details. The information required in this item may change more frequently than the security arrangements in the plan and needs to be updated quickly and easily. The information is not part of the plan because the process required in Part 3 Division 4 for the Director-General to approve changes to maritime security plans is not required for this information. The information is not about the security measures to be implemented and does not require approval by the Director-General.

**Item 29 Details of other maritime industry participants**

This item requires that the port facility operator have contact information for the port security officer and the port service providers who conduct operations within the facility. The port facility operator may need to communicate quickly with those listed should a security incident occur.

**Item 30 Security assessments**

This item requires that security assessments address several key matters. These requirements are consistent with the ISPS code and general risk assessment processes.

This item also requires that the security assessment consider the types of ships and cargoes served by the port facility and any special risks or threats associated with such ships and cargoes to ensure appropriate consideration of risk particular to individual port facilities.

**Item 31 PFSO qualifications and responsibilities**

This item requires that a port facility operator ensure that the port facility security officer (PFSO) has suitable knowledge and skills to perform their responsibilities and provides suitable training to the PFSO. The Director-General will consider the proposed knowledge and training when deciding whether to approve the plan and the records of this training may be subject to audit by an authorised officer.

**Item 32 Other personnel with security role**

This item requires that the port facility operator consider the security responsibilities of employees other than the port facility security officer and ensure that they have appropriate knowledge and receive training. The Director-General will consider the proposed knowledge and training when deciding whether to approve the plan and the records of this training may be subject to audit by an authorised officer.

**Item 33 Matters that must be in plan**

This item requires that the port facility operator address certain matters in their security plan. These matters are based on the requirements of the ISPS Code.

The measures and procedures for these matters should include those identified in the security assessment, including those to take into account special risks or threats associated with the types of ships or their cargoes regularly served by the port.

**Item 34 Consultation**

This item requires that a port facility operator consult with the other maritime industry participants within the port and with its employees. This will ensure that security measures implemented by the various maritime industry participants in a port complement each other, and promote a strong security culture within the port.

**Item 35 Maritime security level 1**

This item requires that the maritime security plan detail the measures to be implemented that are appropriate to the ordinary operating environment for the port facility operator.

The measures and procedures will vary depending on the types and levels of risk identified in the security assessment.

This item also recognises that not all measures in the plan will be implemented immediately. For example, there may be some delay for items requiring major capital investment. In this situation, the maritime security plan should provide that interim measures are in place until the permanent measures can be fully implemented. The Director-General will consider the schedule for implementation and the appropriateness of the interim measures when making the decision to approve a maritime security plan.

**Item 36 Maritime security levels 2 and 3**

This item requires that the maritime security plan include additional security measures that can be implemented during times heightened risk to maritime transport. This reflects the requirement of the ISPS Code for three security levels. The Director-General has the power to change the security level in regulation 17.

**Item 37 Declarations of security**

This item requires that the maritime security plan provide for declarations of security (DOS). The ISPS Code provides for DOS as a way for ports and ships to ensure that security is maintained during a ship/port interface. A ship may agree to a DOS with a port facility operator, or with more than one maritime industry participant within the port, for example the port operator and one or more port service providers may also be party to a DOS.

*Subdivision 2—Form of plan*

**Item 38 Map of port facility**

This item provides more information about the map of the port facility required in regulation 46(2) and (3).

**Item 39 Protection of plan**

This item requires that the port facility operator must protect the maritime security plan from unauthorised access, amendment or disclosure. Preventive security measures and procedures in maritime security plans may be compromised if the plans are disclosed to persons without authority to view or possess them.

***Division 4—Port service providers***

*Subdivision 1—Matters to be dealt with in plan*

**Item 40 Port service provider details**

This item requires that the maritime security plan be accompanied by certain information that identifies the port service provider who owns the plan and their contact details. The information required in this item may change more frequently than the security arrangements in the plan and needs to be updated quickly and easily. The information is not part of the plan because the process required in Part 3 Division 4 for the Director-General to approve changes to maritime security plans is not required for this

information. The information is not about the security measures to be implemented and does not require approval by the Director-General.

**Item 41 Details of other maritime industry participants**

This item requires that the port service provider have contact information for the port security officer and the port facility operators within the port. The port service provider may need to communicate quickly with those listed should a security incident occur.

**Item 42 Security assessments**

This item requires that security assessments address several key matters. These requirements are consistent with the ISPS code and general risk assessment processes.

**Item 43 PSPSO qualifications and responsibilities**

This item requires that a port service provider ensure that the PSPSO have certain knowledge or skills to perform their responsibilities and provides suitable training to the PSPSO. The Director-General will consider the proposed knowledge and training when deciding whether to approve the plan and the records of this training may be subject to audit by an authorised officer.

**Item 44 Other personnel with security role**

This item requires that the port facility operator consider the security responsibilities of employees other than the port service provider security officer and ensure that they have appropriate knowledge and receive training. The Director-General will consider the proposed knowledge and training when deciding whether to approve the plan and the records of this training may be subject to audit by an authorised officer.

**Item 45 Matters that must be in plan**

This item requires that the port service provider address certain matters in their security plan. These matters are based on the requirements of the ISPS code. These measures and procedures for these matters should include these identified in the security assessment.

**Item 46 Consultation**

This item requires that a port service provider consult with the other maritime industry participants within the port and with employees. This will ensure that security measures implemented by the various maritime industry participants in a port complement each other, and promote a strong security culture within the port.

**Item 47 Maritime security level 1**

This item requires that the maritime security plan detail the measures to be implemented that are appropriate to the ordinary operating environment for the port service provider. The measures will vary depending on the type and level of risk identified in the security assessment.

This item also recognises that not all measures in the plan will be implemented immediately. For example, there may be some delay for items requiring major capital

investment. In this situation, the maritime security plan should provide that interim measures are in place until the permanent measures can be fully implemented. The Director-General will consider the schedule for implementation and the appropriateness of the interim measures when making the decision to approve a maritime security plan.

**Item 48 Maritime security levels 2 and 3**

This item requires that the maritime security plan include additional security measures that can be implemented during times heightened risk to maritime transport. This reflects the requirement of the ISPS Code for three security levels. The Director-General has the power to change the security level in regulation 17.

**Item 49 Declarations of security**

This item requires that the maritime security plan provide for declarations of security (DOS). The ISPS Code provides for DOS as a way for ports and ships to ensure that security is maintained during a ship/port interface. A ship may agree to a DOS with a port service provider, or with more than one maritime industry participant within the port, for example the port operator, a port facility and other port service providers may also be party to a DOS.

*Subdivision 2—Form of plan*

**Item 50 Map of port service provider**

This item provides more information about the map of the area under control by a port service provider that is required in regulation 46(2) and (3).

**Item 51 Protection of plan**

This item requires that the port service provider must protect the maritime security plan from unauthorised access, amendment or disclosure. Preventive security measures and procedures in maritime security plans may be compromised if the plans are disclosed to persons without authority to view or possess them.

**PART 4—SHIP SECURITY PLANS AND ISSCS**

***Division 1—Matters to be dealt with in ship security plan***

**Item 52 Identification of ship**

This item requires that a ship security plan be accompanied by a document that lists information about the ship and its operations. The information required in this item may change and need to be updated quickly and easily. The information is not part of the plan because the process required in Part 4 Division 4 for SAMSA to approve ship security plans is not required for this information. The information is not about the security measures to be implemented and does not require approval by SAMSA.

**Item 53 Security assessments**

This item provides that all security assessments must include information about when, how and by whom the security assessment was completed or reviewed and what is covered by the security assessment.

This item also requires that security assessments address key matters. The matters listed here are based the requirements of the ISPS Code.

**Item 54 Ship operator, CSO and SSO**

This item requires that a ship security plan be accompanied by a document that sets out the name of key individuals and contact details for the company security officer.

This item also requires that the ship security plan set out any duties and responsibilities of the CSO and SSO that are in addition to the duties and responsibilities listed in sections 11.2 and 12.2, respectively, of Part A of the ISPS Code.

This item also requires that the ship security plan set out how the CSO will communicate with the master of the ship if the Director-General gives the CSO notice of a change of security level, or a security direction for the ship.

**Item 55 Shore-based personnel and crew with security role**

This item requires that the ship operator consider the security responsibilities of employees other than the ship and company security officer and ensure that they have appropriate knowledge and receive training. SAMSA will consider the proposed knowledge and training when deciding whether to approve the plan and the records of this training will be subject to audit by an authorised officer.

**Item 56 Training**

This item requires that a ship operator plan for and provide suitable training to the company, ship security officers and crew and shore based personnel with security responsibilities. SAMSA will consider the proposed knowledge and training when deciding whether to approve the plan and the records of this training will be subject to audit by an authorised officer.

**Item 57 Matters that must be in plan**

This item requires that the ship operator address certain matters in their security plan. These matters are based on the requirements of the ISPS Code. The measures and procedures for these matters should include those identified in the security assessment.

**Item 58 Maritime security level 1**

This item requires that the ship security plan detail the measures that will be implemented that are appropriate to the ordinary operating environment for the ship. The types of measures will vary depending on the level of risk identified in the security assessment.

This item also recognises that not all measures in the plan will be implemented immediately. For example, there may be some delay for items requiring major capital investment. In this situation, the ship security plan should provide that alternative measures are in place until the permanent measures can be fully implemented. SAMSA

will consider the schedule for implementation and the appropriateness of the alternative measures when making the decision to approve a ship security plan.

**Item 59 Maritime security levels 2 and 3**

This item requires that the ship security plan include additional security measures that can be implemented during times of heightened risk to maritime transport. This reflects the requirement of the ISPS Code for three security levels. The Director-General has the power to change the security level in regulation 17.

**Item 60 Declarations of security**

This item requires that the ship security plan provide for declarations of security (DOS). The ISPS Code provides for DOS as a way for ports and ships to ensure that security is maintained during a ship/port interface. A ship may request a DOS from a port it is visiting, but the port is not required under the ISPS Code to agree to a DOS.

**Item 61 Security of ship in non-ISPS Code compliant ports**

This item requires that the ship security plan for a ship that may call at non-ISPS Code compliant ports or locations plan for the maintenance of security measures that will protect the ship from any security risks associated with those locations.

**Item 62 Security of ship in exceptional circumstances**

This item requires that a ship security plan provide for the ongoing security of the ship during exceptional circumstances. Ships are vulnerable to sudden changes of route and activity due, for example, to bad weather, search and rescue obligations and the security of the ship should be maintained at such times.

**Item 63 Pre-entry information**

This item requires that a ship security plan address how certain ships will provide specified pre-entry information. The pre-entry information is based on the requirements of SOLAS regulation XI-2/9.2.

**Item 64 Maritime transport security incidents**

This item requires that the ship security plan address how maritime transport security incidents will be reported to SAMSA.

This item also requires that a maritime security plan address procedures for responding to security threats or breaches of security, including maintaining operations. This item ensures that, in an emergency, the appropriate course of action is understood and followed.

**Item 65 Security equipment**

This item requires that a ship security plan list the security equipment on board the ship and provide for the maintenance of that equipment in a calibrated state.

**Item 66 On-board systems**

This item requires that a ship security plan provide information about specified systems carried on the ship that may have a security function.

This item also requires, if a ship has a ship security alert system, that the plan address the characteristics and correct use of the alert.

The requirement to have a ship security alert system is set out in regulation 113.

**Item 67 Ship security records**

This item requires that the ship security plan list the ship security records that must be kept on the ship and plan for preserving those records, and providing them to a port state for inspection. A port state control officer may inspect certain ship security records under SOLAS regulation XI-2/9.

**Item 68 Security plan audits and reviews**

This item provides that a ship security plan must include information about when the security plan will be audited and reviewed, and the procedure for conducting the audit or review. It is important that ship security plans are subject to ongoing independent audit and review to ensure that they remain adequate and relevant.

***Division 2—Form of ship security plan***

**Item 69 Statement about authority of master**

This item requires that a ship security plan include a statement preserving the authority of the master on the ship. This reflects the obligation on shipping companies in section 6.1 of Part A of the ISPS Code.

**Item 70 Protection of plan**

This item requires that the ship operator must protect the ship security plan from unauthorised access, amendment or disclosure. Preventive security measures and procedures in ship security plans may be compromised if the plans are disclosed to persons without authority to view or possess them.

## ANNEX 3—FEES

This Annex will prescribe the fees payable to the Director-General in respect of the exercise of certain functions by the Director-General.



Printed by and obtainable from the Government Printer, Bosman Street, Private Bag X85, Pretoria, 0001
Gedruk deur en verkrygbaar by die Staatsdrukker, Bosmanstraat, Privaatsak X85, Pretoria, 0001

26166—1