Maritime Transport Security Regulations 2003 2003 No. 366

EXPLANATORY STATEMENT
Statutory Rules 2003 No. 366

Issued by Authority of the Minister for Transport and Regional Services

Subject: *Maritime Transport Security Act 2003*

Maritime Transport Security Regulations 2003

Section 209 of the *Maritime Transport Security Act 2003* (the Act) provides that the Governor General may make Regulations prescribing matters:

(a) required or permitted by this Act to be prescribed; or

(b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

The Act gives effect in Australian law to a new international maritime security regime, which comes into force on 1 July 2004. The new regime is set out in the new Chapter XI-2 of the Safety of Life at Sea (SOLAS) Convention and the International Ship and Port Facilities (ISPS) Code.

Attachment A lists the various provisions in the Act that provide for the scope of regulations made under the Act.

These Regulations are the first tranche of the regulations that must be made to give effect to the Act. The first tranche establishes the key requirements for Australian Maritime Industry Participants (MIPs). This assists Australian MIPs to have maritime security plans written, approved and implemented by 1 July 2004, as required by the SOLAS Convention. The second tranche of the Regulations will be prepared early in 2004.

The Regulations provide detail about the obligations on MIPs with regard to the content and form of their security assessments and plans; the role of security officers; sharing security information; establishing and enforcing security zones; screening and clearing passengers and negotiating declarations of security. Other MIPs who are required to have a maritime security plan are identified. The Regulations also create an obligation on operators of regulated Australian ships to provide pre-entry information when they return to Australia from an overseas voyage, and to provide a ship security alert system.

The Regulations identify what is a weapon and what is a prohibited item and create exemptions from some weapons provisions in the Act.

The Regulations also create an obligation on the Secretary of the Department of Transport and Regional Services to consult with certain people when giving a security or control direction under the Act and when it is reasonable and practicable to do so.

Details of the Regulations are set out in Attachment B.

The Act specifies no conditions that need to be met before the power to make the Regulations may be exercised.

The Regulations commence in two stages. The first stage commenced on 1 January 2004 and comprises Part 1, Part 3 (except Subdivision 3.4.1), Part 4, regulations 6.05, 6.20, 6.80, 6.85, 6.105, Part 12 and Part 13. This will assist the Australian maritime industry in developing maritime and ship security plans to achieve compliance with international requirements by 1 July 2004. All other provisions of the Regulations are not required in the initial plan development and approval phase and will commence on the commencement of Part 2 of the Act. It is anticipated that Part 2 of the Act will commence on 1 July 2004, at the same time as the ISPS Code comes into effect internationally.

ATTACHMENT A

Sections of the Act referring to making regulations

Section 10 of the Act provides that the Regulations may prescribe

- a person who conducts a maritime related enterprise as a maritime industry participant (MIP);

- documents as `ship security records';

- a thing as a weapon or prohibited item

Subsection 33(5) of the Act provides that the Regulations may prescribe requirements for, or in relation to the giving of security directions.

Section 42 of the Act provides that the regulations may prescribe maritime industry participants who must have a maritime security plan.

Paragraphs 47(2)(b) and 66(2)(b) of the Act provide that regulations may be made listing matters which must be addressed in the security assessment. Sections 48 and 67 provide that regulations may be made prescribing content for maritime and ship security plans. Paragraphs 49(1)(b) and 68(b) provides that the regulations may prescribe requirements for the preparation of maritime and ship security plans.

Subsection 99(7) of the Act provides that the Regulations may prescribe requirements for, or in relation to, the giving of control directions.

Section 103 provides that the Regulations may prescribe different types of port security zones and section 105 provides that the Regulations may prescribe requirements for the port security zones, including penalties for offences against the Regulations.

Section 107 provides that the Regulations may prescribe different types of ship security zones and section 109 provides that the Regulations may prescribe requirements for the ship security zones, including penalties for offences against the Regulations.

Section 110 provides that the Regulations may prescribe different types of on-board security zones and section 113 provides that the Regulations may prescribe requirements for the on-board security zones, including penalties for offences against the Regulations.

Section 119 provides that the Regulations may prescribe requirements for screening and clearing and the circumstances in which persons, goods, vehicles or vessels are required to be cleared. Subsections 115(2) and 116(2) provide that the regulations may exempt people and goods from certain screening and clearing requirements.

Subparagraphs 120(1)(c)(iii) and 120(3)(c)(iii) provide that the Regulations may authorise a person to have a weapon in his or her possession in a maritime security zone. Subparagraphs 121(1)(c)(ii) and 121(3)(c)(ii) provide that the Regulations may authorise a person to pass through a screening point with a weapon in their possession. Subsections 122(d) and 123(d) provide that the Regulations may authorise a person to have a weapon on board a regulated Australian ship.

Subsection 126(a) provides that the Regulations may prescribe requirements in relation to the carriage and use of weapons in a maritime security zone or on board a regulated Australian ship.

Subparagraphs 127(1)(d)(iii) and 127(3)(d)(iii) provide that the Regulations may authorise a person to have a prohibited item in his or her possession in a maritime security zone. Subparagraphs 128(1)(c)(ii) and 128(3)(c)(ii) provide that the Regulations may authorise a person to pass through a screening point with a prohibited item in their possession. Subsections 129(d) and 130(d) provide that the Regulations may authorise a person to have a prohibited item on board a regulated Australian ship.

Subsection 133(a) provides that the Regulations may prescribe requirements in relation to the carriage and use of prohibited in a maritime security zone or on board a regulated Australian ship.

ATTACHMENT B

Details of the proposed Maritime Transport Security Regulations 2003

Part 1 Preliminary

1.01 Name of Regulations

This regulation provides that these regulations are to be cited as the *Maritime Transport Security Regulations 2003*.

1.02 Commencement

This regulation provides that parts of the regulations commence on 1 January 2004, and the remainder of the regulations commence at the same time as commencement of Part 2 of the Act. The provisions commencing on 1 January 2004 are those relating to the content and form of the security plans, the preliminary provisions, the types of maritime security zones and the requirement to have a ship security alert.

This two stage commencement allows for development and approval of maritime and ship security plans before the international deadline of 1 July 2004 for implementation of the International Ship and Port Facility Security Code (the ISPS Code). The other provisions will not be required until the commencement of the ISPS Code on 1 July 2004.

1.03 Definitions

This regulation defines many terms used in these regulations. Unless otherwise stated, a term used in these regulations has the same meaning as in the ISPS Code.

1.04 Purposes of these Regulations

This regulation describes the purposes of these regulations. The purposes are to:

a) ensure that maritime and ship security plans address specific matters;

b) ensure that the requirements for maritime and ship security plans are clearly set out;

c) require that the Secretary consult with certain people when he gives a security or control direction;

d) identify types of ship, port and on-board security zones;

e) specify requirements for screening and clearing;

f) identify certain things as weapons and prohibited items for the purposes of the Act.

1.05 Port service providers

This regulation provides that lighter or barge operators, line handling operators, pilot boat operators and tug operators are maritime industry participants (MIPs). These people have been prescribed because of their role in providing services to security regulated ships on the water, without passing through any land-side security arrangements in a port facility to gain access to

the ship. The prescribed MIPs are required to submit a maritime security plan under regulation 3.175.

1.10 Company security officers

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

Subregulation (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.

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

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

1.15 Ship security officers

This regulation 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.

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

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

Subregulation (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 regulation 4.110 of these regulations.

1.20 Port security officers

This regulation requires that the port operator designate a port security officer (PSO) before submitting the port security plan to the Secretary.

Subregulation (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.

Subregulation (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.

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

1.25 Port facility security officers

This regulation requires that the port facility operator designate a port facility security officer (PFSO) before submitting the port facility security plan to the Secretary for approval.

Subregulation (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.

Subregulation (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.

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

1.30 Port service provider security officers

This regulation requires that the port service provider designate a port service provider security officer (PSPSO) before submitting the port service provider security plan to the Secretary for approval.

Subregulation (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.

Subregulation (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.

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

1.35 Delegation by security officers

This regulation 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.

1.40 Shore-based personnel and crew

This regulation 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.

1.45 Declarations of security

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

1.50 Security plan audits and reviews

This regulation 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 security plan, and may be an offence under section 44 of the Act.

Subregulation (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.

Subregulation (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 a maritime security inspector.

1.55 Ship security records

This regulation requires that a regulated Australian ship keep certain information. This list is based on section 9.2 of Chapter XI-2 of the SOLAS Convention. 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 a maritime security inspector.

1.60 Prohibited items

This regulation provides a definition of `prohibited item' for the purposes of section 10 of the Act.

1.65 Weapon

This regulation and the accompanying table provide a definition of a weapon for the purposes of section 10 of the Act. The definition excludes certain safety devices that must be carried in the ship and accessible to those on board the ship.

1.70 Water-side restricted zone

This regulation provides information about where the Secretary may establish a type of port security zone called a `water-side restricted zone'.

Part 2 Maritime security levels and security directions

Division 2.1 Preliminary

The text under this heading is a note indicating that this Division heading is reserved for future use.

Division 2.2 Maritime security levels

The text under this heading is a note indicating that this Division heading is reserved for future use. This Division will be inserted in the second tranche of regulations.

Division 2.3 Security directions

2.30 Requirement for consultation

This regulation requires that where reasonable and practicable the Secretary must consult with 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 MIPs, the harbour master and the port security officer, the Secretary will be made aware of any safety implications of his directions.

The Secretary is also required to consult with Commonwealth, State and Territory agencies whose operations may be affected by the control direction. This recognises that a number of agencies operate in ports, and many agencies have an interest in the movement of ships, for example the Australian Customs Service must provide clearance before a ship can leave an Australian port on an overseas voyage.

2.35 Communicating security directions

This regulation provides that the Secretary may give, communicate or revoke a security direction by facsimile or e-mail. This is in addition to subsection 33(4) of the Act which allows a security direction to be given in writing or orally.

This regulation allows a port or ship operator to use the same communication methods as the Secretary.

Part 3 Maritime security plans

Division 3.1 Preliminary

3.05 Common requirements for security assessments

This regulation 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.

3.10 Common requirements for security plan audits and reviews

This regulation 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 continue to contribute to the *maritime security outcomes* in subsection 3(4) of the Act.

3.15, 3.20, 3.25 Port operator, Port facility operator and Port service provider to give information

These regulations provide that a port operator, port facility operator and port service provider must share certain information with other MIPs within the port. It is important that MIPs 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 subregulations 3.60, 3.130 and 3.215.

Division 3.2 Port operators

Subdivision 3.2.1 Matters to be dealt with in the plan

3.30 General

This regulation 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 declared by the Secretary under section 13 of the Act.

3.35 Port operator details

This regulation 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 regulation 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 5 of the Act for the Secretary 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 Secretary.

3.40 Security assessments

This regulation requires that security assessments address several key matters. These requirements are consistent with the ISPS Code and general risk assessment, such as the Australian and New Zealand Risk Management Standard 4360:1999. The matters also reflect the port operator's role in the identification of port-wide gaps in security that require treatment.

3.45 Port security officer qualifications and responsibilities

This regulation requires that a port operator ensures 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 Secretary will consider the proposed knowledge and training when deciding whether to approve the plan. Records of training undertaken may be subject to audit by the Department.

3.50 Other personnel with security role

This regulation 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 Secretary 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 the Department.

3.55 Matters that must be in plan

This regulation 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.

3.60 Consultation and communication

This regulation requires that a port operator consult with the other maritime industry participants within the port and with employees. (Note that the Act provides that employee includes contractors.) This will ensure that security measures implemented by the various MIPs in a port complement each other, and promote a strong security culture within the port.

Subregulation (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.

3.65 Maritime security level 1

This regulation 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.

Subregulation (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 Secretary will consider the

schedule for implementation and the appropriateness of the interim measures when making the decision to approve a maritime security plan.

3.70 Maritime security levels 2 and 3

This regulation 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 Secretary has the power to change the security level in section 22 of the Act.

3.75 Declarations of security

This regulation 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 MIP within the port, for example a port facility operator and one or more port service providers may also be party to a DOS.

3.80 Water-side restricted zones

This regulation requires that the port operator must give the Secretary certain information about the need for a water-side restricted zone and the way the zone will be maintained, including access control measures to ensure the integrity of the zone. The Secretary requires this information to ensure that the establishment of zones will help achieve the maritime security outcomes. Zones can be put in place to suit local conditions and they are flexible security arrangements.

The Secretary may establish maritime security zones that are in force only at certain times or when certain conditions are met. For example, a zone may be in force only when a ship or type of ship is present in the port. The location of zones and measures to deter and detect unauthorised access will be informed by security assessments.

3.85 Ship security zones

This regulation requires that a maritime security plan for a port operator demonstrate how the port operator will monitor and control unauthorised access to ship security zones should they be declared. These zones may be declared around particular ships or types of ships and can move with the ship within the boundaries of the security regulated port.

Subdivision 3.2.2 Form of plan

3.90 Map of port

This regulation requires that a port operator provide a map or maps that meet the requirements in subsections 49(2) and (3) of the Act.

3.95 Protection of plan

This regulation 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 3.3 Port facility operators

Subdivision 3.3.1 Matters to be dealt with in plan

3.100 Port facility operator details

This regulation 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 regulation 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 5 of the Act for the Secretary 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 Secretary.

3.105 Details of other maritime industry participants

This regulation 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.

3.110 Security assessments

This regulation requires that security assessments address several key matters. These requirements are consistent with the ISPS code and general risk assessment processes such as the Australian and New Zealand Risk Management Standards 4360:1999.

This regulation 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.

3.115 PFSO qualifications and responsibilities

This regulation 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 Secretary 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 the Department.

3.120 Other personnel with security role

This regulation 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 Secretary 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 the Department.

3.125 Matters that must be in plan

This regulation 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.

3.130 Consultation

This regulation requires that a port facility operator consult with the other maritime industry participants within the port and with its employees. (Note that the Act provides that employee includes contractors.) This will ensure that security measures implemented by the various MIPs in a port complement each other, and promote a strong security culture within the port.

3.135 Maritime security level 1

This regulation 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 regulation 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 Secretary will consider the schedule for implementation and the appropriateness of the interim measures when making the decision to approve a maritime security plan.

3.140 Maritime security levels 2 and 3

This regulation 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 Secretary has the power to change the security level in section 22 of the Act.

3.145 Declarations of security

This regulation 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 MIP within the port, for example the port operator and one or more port service providers may also be party to a DOS.

3.150 Land-side restricted zones

This regulation requires that the port facility operator provide to the Secretary certain information about the need for a land-side restricted zone, and the way the zone will be managed. The Secretary requires this information to ensure that the establishment of the zone will help achieve the maritime security outcomes. Zones can be put in place to suit local conditions and they are flexible security arrangements.

The Secretary may establish maritime security zones that are in force only at certain times or when certain conditions are met. For example, a zone may be in force only when a ship or type of ship is being loaded or unloaded at the berth. The location of zones and measures to deter and detect unauthorised access will be informed by security assessments.

3.155 Cleared zones

This regulation requires that the port facility operator include measures for screening persons and goods before they are introduced into a cleared zone. Not all port facilities will have cleared zones. Port facilities that serve passenger ships, and port facilities that identify screening and clearing in their security assessments as a security measure they wish to use, may ask the Secretary to establish cleared zones to facilitate screening and clearing.

3.160 Passenger ships

This regulation requires that operators of port facilities used to load and unload passenger ships must include in their maritime security plans procedures for screening and clearing persons and detecting and dealing with weapons and prohibited items. The maritime security plan must identify the person or persons responsible for these measures. The screening and clearing function may be contracted to an external service provider.

Subdivision 3.3.2 Form of plan

3.165 Map of port facility

This regulation provides more information about the map of the port facility required in subsection 49(2) of the Act.

3.170 Protection of plan

This regulation 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 3.4 Port service providers

Subdivision 3.4.1 Preliminary

3.175 Participants required to have maritime security plans

This regulation identifies the maritime industry participants required to have a maritime security plan, in addition to those listed in section 42 of the Act.

3.180 Certain port service providers not required to have maritime security plans

This regulation provides that a port service provider need not have a maritime security plan if the port service provider has agreed in writing with a port operator to have the activities of the port service provider covered by the maritime security plan of the port operator. The Act provides for this arrangement in subsection 45(3).

Subdivision 3.4.2 Matters to be dealt with in plan

3.185 Port service provider details

This regulation 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 regulation 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 5 for the Secretary 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 Secretary.

3.190 Details of other maritime industry participants

This regulation 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.

3.195 Security assessments

This regulation requires that security assessments address several key matters. These requirements are consistent with the ISPS code and general risk assessment processes such as the Australia/New Zealand Risk Management Standard 4360:1999.

3.200 PSPSO qualifications and responsibilities

This regulation 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 Secretary 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 the Department.

3.205 Other personnel with security role

This regulation 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 Secretary 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 the Department.

3.210 Matters that must be in plan

This regulation 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.

3.215 Consultation

This regulation requires that a port service provider consult with the other maritime industry participants within the port and with employees. (Note that the Act provides that employee includes contractors.) This will ensure that security measures implemented by the various MIPs in a port complement each other, and promote a strong security culture within the port.

3.220 Maritime security level 1

This regulation 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 regulation 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 Secretary will consider the schedule for implementation and the appropriateness of the interim measures when making the decision to approve a maritime security plan.

3.225 Maritime security levels 2 and 3

This regulation 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 Secretary has the power to change the security level in section 22 of the Act.

3.230 Declarations of security

This regulation 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 MIP within the port, for example the port operator, a port facility and other port service providers may also be party to a DOS.

3.235 Port security zones

This regulation requires that the port service provider give to the Secretary certain information about the need for a port security zone, and the way the zone will be managed. The Secretary requires this information to ensure that the establishment of the zone will help achieve the maritime security outcomes. Zones can be put in place to suit local conditions and they are flexible security arrangements.

The Secretary may establish port security zones that are in force only at certain times or when certain conditions are met. For example, a zone may be in force only when the port service provider is conducting certain operations.

The location of zones and measures to deter and detect unauthorised access will be informed by security assessments.

Part 6 of the Act provides that zones can only be established within the boundaries of a security regulated port. This will exclude areas controlled by port service providers based outside the security regulated port.

Subdivision 3.4.3 Form of plan

3.240 Map of port service provider

This regulation provides more information about the map of the area under control by a port service provider that is required in subsection 49(2) of the Act.

3.245 Protection of plan

This regulation 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 4.1 Preliminary

The text under this heading is a note indicating that this Division heading is reserved for future use.

Division 4.2 Matters to be dealt with in ship security plan

4.20 Identification of ship

This regulation 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 regulation 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 5 for the Secretary 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 the Secretary.

4.25 Security assessments

This regulation 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 regulation also requires that security assessments address key matters. The matters listed here are based on the Australia/New Zealand standard for risk assessment (4360:1999) and the requirements of the ISPS Code.

4.30 Ship operator, CSO and SSO

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

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

4.35 Shore-based personnel and crew with security role

This regulation 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. The Secretary 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 the Department.

4.40 Training

This regulation 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. The Secretary 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 the Department.

4.45 Matters that must be in plan

This regulation 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.

4.50 Maritime security level 1

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

4.55 Maritime security levels 2 and 3

This regulation requires that the ship security plan includes 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 Secretary has the power to change the security level in section 22 of the Act.

4.60 Declarations of security

This regulation 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.

4.65 On-board security zones

This regulation requires that the ship operator must give the Secretary certain information about the need for an on-board security zone and the way the zone will be managed. The Secretary requires this information to ensure that the establishment of the zone will help achieve the maritime security outcomes. Zones can be put in place to suit conditions on each ship and they are flexible security arrangements.

The Secretary may establish on-board security zones that are in force only at certain times or when certain conditions are met, for example a zone may be in force only when the ship is in a port.

4.70 Security of ship in non-ISPS Code compliant ports

This regulation requires that the ship security plan for a ship which 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.

4.75 Security of ship in exceptional circumstances

This regulation 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.

4.80 Pre-entry information

This regulation 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 regulation 9.2 of Chapter XI-2 of the SOLAS Convention.

4.85 Maritime transport security incidents

This regulation requires that the ship security plan address how maritime transport security incidents will be reported to the Secretary. Information is an important tool in the maritime security regime. Requiring this information in the plan will increase awareness of the reporting obligation in the Act and improve compliance with this part of the Act.

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

4.90 Security equipment

This regulation 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.

4.95 On-board systems

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

This regulation also requires that 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 13.05.

4.100 Ship security records

This regulation 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 regulation 9 of chapter XI-2 of the SOLAS Convention.

4.105 Security plan audits and reviews

This regulation 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 continue to contribute to the *maritime security outcomes* in subsection 3(4) of the Act.

Division 4.3 Form of ship security plan

4.110 Statement about authority of master

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

4.115 Protection of plan

This regulation 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.

Part 5 Regulated foreign ships

Division 5.1 Obligations

The text under this heading is a note indicating that this Division heading is reserved for future use. This Division will be inserted in the second tranche of regulations.

Division 5.2 Control Directions

5.20 Requirement for consultation

This regulation requires that where reasonable and practicable the Secretary must consult with certain people about control directions. The Secretary has broad powers to order the movement of regulated foreign ships under section 99 of the Act. 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 MIPs, the harbour master and the port security officer, the Secretary will be made aware of any safety implications of his or her directions.

The Secretary is also required to consult with Commonwealth, State and Territory agencies whose operations may be affected by the control direction. This recognises that a number of agencies operate in ports, and many agencies have an interest in the movement of ships, for example the Australian Customs Service must provide clearance before a ship can leave an Australian port on an overseas voyage.

5.25 Communicating control directions

This regulation allows the Secretary to communicate a control direction by facsimile or by e-mail. This is in addition to section 99(5) of the Act which provides that a control direction must be committed to writing and may be communicated orally.

Part 6 Maritime security zones

Division 6.1 Preliminary

6.05 Access by certain persons not be denied

This regulation protects the right of certain people to enter a port or an area within a port when they are exercising powers under laws other than the Act. For example, customs, quarantine and police officers all work within ports, and it is not the intention of this regulation to prevent their access. This regulation clarifies the intention of the Act and regulations not to stop existing government and police activities in ports.

Division 6.2 Port security zones

Subdivision 6.2.1 General

6.20 Types of port security zones

This regulation identifies the different types of port security zones that may be established by the Secretary within a security regulated port. The terms are defined in Part 1 of the regulations.

6.25 Security barriers

This regulation provides a definition of ***security barrier*** by describing the key purposes of a security barrier, defining the boundary of a zone and deterring unauthorised access into the zone. The regulation provides some examples of security barriers on land and on water.

Subregulation (2) imposes some additional requirements for land-side security zones.

Subdivision 6.2.2 Land-side restricted zones

6.30 Identification of zones

This regulation requires that a land-side restricted zone be clearly identifiable. This serves three purposes. Firstly, a clearly identifiable boundary is a better security outcome because it will help personnel with security responsibilities identify unauthorised access to the zone. Secondly, it is important that members of the public are made aware of the boundaries of zones because of the criminal penalties attached to unauthorised entry into a zone. Thirdly, advising people of the penalties for unauthorised access to a zone will reduce the incidence of unauthorised entry.

6.35 Duties of port facility operator

This regulation makes it a strict liability offence for a port facility operator to fail to control access to a land-side restricted zone within the port facility. The access control measures will generally be in the maritime security plan of the port facility operator and subject to the offence for breach of maritime security plan in the Act, however zones may also be established by the Secretary independent of the maritime security plans, and so a separate offence is required.

6.40 Duties of port service provider

This regulation makes it a strict liability offence for a port service provider to fail to control access to a maritime security zone within the boundaries of the area under the control of the port service provider. The access control measures will generally be in the maritime security plan of the port service provider and subject to the offence for breach of maritime security plan in the Act, however zones may also be established by the Secretary independent of the maritime security plans, and so a separate offence is required.

6.45 Offences -- unauthorised entry

This regulation makes it a strict liability offence for a person to enter or remain in a land-side restricted zone unless authorised to do so. This regulation also makes it a strict liability offence to take into or leave a vehicle or thing in a land-side restricted zone unless authorised to do so.

Subdivision 6.2.3 Cleared zones

6.50 Duties of port facility operator

This regulation requires that a port facility operator ensure that a cleared zone is checked for unauthorised persons, goods, vehicles and vessels before the zone comes into force.

This ensures that any person screened and cleared to enter the zone cannot access weapons and prohibited items from within the zone.

Subregulation (2) provides that it is the responsibility of the port facility operator to screen and clear people and goods before they enter the cleared zone.

6.55 Identification of zones

This regulation requires that a cleared zone be clearly identifiable. This serves three purposes. Firstly, a clearly identifiable boundary is a better security outcome because it will help personnel with security responsibilities identify unauthorised access to the zone. Secondly, it is important that members of the public are made aware of the boundaries of zones because of the criminal penalties attached to unauthorised entry into a zone. Thirdly, advising people of the penalties for unauthorised access to a zone will reduce the incidence of unauthorised entry.

6.60 Offences -- unauthorised entry

This regulation makes it a strict liability offence for a person to enter or remain in a cleared zone if they have not been screened and cleared. Subregulation (2) makes it a strict liability offence to take or leave a vehicle, vessel or thing in a cleared zone if it has not been screened and cleared. Screening and clearing is a condition of entry into a cleared zone.

Subdivision 6.2.4 Water-side restricted zones

6.65 Identification of zones

This regulation requires that a water-side restricted zone be clearly identifiable. This serves three purposes. Firstly, a clearly identifiable boundary is a better security outcome because it will help personnel with security responsibilities identify unauthorised access to the zone. Secondly, it is important that members of the public are made aware of the boundaries of zones because of the criminal penalties attached to unauthorised entry into a zone. Thirdly, advising people of the penalties for unauthorised access to a zone will reduce the incidence of unauthorised entry.

It is difficult to clearly delineate a boundary on the water, and the regulation suggests some possible measures.

6.70 Duties of port operator

This regulation requires that a port operator take steps to advise the public of the existence of a water-side restricted zone. Land-side restricted zones are identified to the public at the boundary of the zone by a security barrier and signs. This is not practical for a zone on the water, so the public must be advised of the location of the zones and the consequences of unauthorised entry into the zone before they reach the zone, and possibly before they enter the port. This advice could be given by advertising the location and requirements of the zone in the media or by signage around the port.

This regulation makes it a strict liability offence for a port operator to fail to monitor access to a water-side security zone. The obligation is less than the obligation to control access to a land-side restricted zone in regulation 6.35 because of the physical difficulty of controlling access on the water.

The access control measures will generally be in the maritime security plan of the port operator and subject to the offence for breach of maritime security plan in the Act, however zones may also be established independently of the maritime security plans, and so a separate offence is required.

6.75 Offences -- unauthorised entry

This regulation makes it a strict liability offence for a person to enter or remain in a water-side restricted zone if they are not authorised to be in the zone. Subregulation (2) makes it a strict liability offence to take into or leave a vessel or thing in water-side restricted zone without authorisation.

Division 6.3 Ship security zones

6.80 Exclusion zones

This regulation provides that an exclusion zone is a type of ship security zone.

6.85 Declaration of operation of zone

This regulation provides that a port operator may request that the Secretary establish a ship security zone around a particular ship while the ship is in the port.

This regulation requires that the port operator must give the Secretary certain information about the need for an exclusion zone and the way the zone will be managed, including access control measures. The Secretary requires this information to ensure that the establishment of zones will help achieve the maritime security outcomes. Zones can be put in place to suit local conditions and they are flexible security arrangements.

6.90 Identification of zones

This regulation requires that a ship security zone be clearly identifiable, that the public are aware that access to the zone is controlled and the penalty for unauthorised access. This serves three purposes. Firstly, a clearly identifiable boundary is a better security outcome because it will help personnel with security responsibilities identify unauthorised access to the zone. Secondly, it is important that members of the public are made aware of the boundaries of zones because of the criminal penalties attached to unauthorised entry into a zone. Thirdly, advising people of the penalties for unauthorised access to a zone will reduce the incidence of unauthorised entry.

A ship security zone will be identified as an area within a specified distance from the ship. Land-side restricted zones are identified to the public at the boundary of the zone by a security barrier and by signs. This is not practical for a zone on the water, so the public must be advised of the existence of the zones and the consequences of unauthorised entry into the zone before they reach the zone, and possibly before they enter the port. This advice could be given by advertising the location and requirements of the zone in the media or by signage around the port.

6.95 Duties of port operator

This regulation makes it a strict liability offence for a port operator to fail to monitor access to a ship security zone. The obligation is less than the obligation to control access to a land-side restricted zone in regulation 6.35 because of the physical difficulty of controlling access on the water.

The access control measures will generally be in the maritime security plan of the port operator and subject to the offence for breach of maritime security plan in the Act, however zones may also be established by the Secretary independent of the maritime security plans, and so a separate offence is required.

6.100 Offences -- unauthorised entry

This regulation makes it a strict liability offence for a person to enter or remain in a ship security zone if they are not authorised by the port operator to be in the zone. Sub-regulation (2) makes it a strict liability offence to take into or leave a vessel or thing in a ship security zone without authorisation.

Division 6.4 On-board security zones

6.105 On-board restricted areas

This regulation provides that an on-board restricted area is a type of on-board security zone that may be established by the Secretary.

6.110 Identification of zones

This regulation requires that an on-board security zone be clearly identifiable. This serves three purposes. Firstly, a clearly identifiable boundary is a better security outcome because it will help personnel with security responsibilities identify unauthorised access to the zone. Secondly, it is important that members of the public are made aware of the boundaries of zones because of the criminal penalties attached to unauthorised entry into a zone. Thirdly, advising people of the penalties for unauthorised access to a zone will reduce the incidence of unauthorised entry.

6.115 Duties of ship operators

This regulation makes it a strict liability offence for a ship operator to fail to control access to an on-board security zone on a ship they operate. The access control measures will generally be in the ship security plan for the ship and subject to the offence for breach of ship security plan in the Act, however zones may also be established by the Secretary independent of the ship security plans, and so a separate offence is required.

6.120 Offences -- unauthorised entry

This regulation makes it a strict liability offence for a person to enter or remain in a on-board security zone if they are not authorised by the ship operator to be in the zone. Sub-regulation (2) makes it a strict liability offence to take or leave goods or other things in an on-board security zone without authorisation.

Part 7 Other security measures

Division 7.1 Preliminary

7.05 Access by certain persons not be denied

This regulation protects the existing rights of certain authorised people to enter a port or an area within a port when they are exercising powers under laws other than the Act. For example, customs, quarantine and police officers all work within ports, and it is not the intention of this regulation to stop their existing access. This regulation clarifies the intention of the Act not to interfere with existing government and police activities in ports.

Division 7.2 Screening and clearing

7.20 Duties of port facility operator

This regulation requires the port facility operator to ensure proper screening and clearing of persons and baggage. This regulation is subject to exemptions that are outlined in regulation 7.25. Screening and clearing is a condition of entry into a cleared zone.

7.25 Persons who need not be screened

This regulation provides more information about the persons that are exempted from the process of screening and clearing under paragraphs 115(2)(b) and (c) of the Act.

Subregulation 7.25(3) recognises the need for certain persons to be able to move freely around the port at security level 1. For example, a crewmember of a passenger ship needs free access to the ship interface as the ship is their home. Also, maritime security officers have been exempted from screening and clearing as they have security responsibilities. Various government officials have also been exempted as it is the intention of the Act not to interfere with existing government and police activities in ports as stipulated in regulation 7.05.

In subregulation 7.25(4) the exemptions from clearing and screening at security levels 2 and 3 have been limited to those persons that may need immediate access. In a heightened threat environment, the exemptions have been preserved for those officials that may need to respond to a potential breach of security or emergency.

7.30 Equipment to be used for screening

This regulation requires that the equipment to be used for screening must be capable of detecting weapons and prohibited items on persons or in their baggage. This regulation also provides details of the kind of equipment that could be used for this purpose.

7.35 Offences -- screening and clearing

This regulation requires that a port facility or a ship operator must not allow a person or baggage that requires screening to pass through a screening point without being screened and cleared.

Division 7.3 Weapons and prohibited items

7.40 Persons authorised to carry weapons or prohibited items in cleared zones

This regulation identifies certain persons who may carry weapons or prohibited items in cleared zones without committing an offence under sections 120 and 127 of the Act.

This regulation recognises that certain persons in the port will need to handle or carry weapons or prohibited items in a cleared zone for purposes related to their duties.

Subregulation (3) recognises the need for certain persons to be authorised to have a weapon or a prohibited item in a cleared zone for the purpose of carrying it onto a ship to be secured during a voyage. This acknowledges that passengers may have weapons or prohibited items that will need to be secured for the length of the voyage for example, a spear fishing gun or gun used for hunting.

4.45 Authorised possession of weapons or prohibited items when passing through screening points

This regulation ensures that a member of the Australian Defence Force (ADF) does not commit an offence under sections 121 and 128 of the Act by passing through a screening point with a weapon or prohibited item.

Sections 120 and 127 of the Act authorise members of the ADF to carry weapons or prohibited items in a maritime security zone. The intention of this is to ensure that members of the ADF do not commit an offence by carrying a weapon or prohibited item into a zone when they are allowed to have the weapon or prohibited item once in the zone.

7.50 Authorised carriage or possession of weapons or prohibited items on board regulated Australian ships

This regulation identifies certain persons that may carry or possess a weapon or prohibited item on board a regulated Australian ship without committing an offence under sections 122, 123, 129 and 130 of the Act.

Sections 122, 123, 129 and 130 of the Act make it an offence if a person has a weapon or prohibited item on board a regulated Australian ship unless that person is authorised by the regulations to do so.

This regulation recognises that certain persons on a security regulated ship may need to carry a weapon or a prohibited item for purposes related to their duties.

Part 8 Powers of officials

Division 8.1 Preliminary

The text under this heading is a note indicating that this Division heading is reserved for future use.

Division 8.2 Maritime security inspectors

The text under this heading is a note indicating that this Division heading is reserved for future use. This Division will be inserted in the second tranche of regulations.

Division 8.3 Duly authorised officers

The text under this heading is a note indicating that this Division heading is reserved for future use.

Division 8.4 Law enforcement officers

8.40 Customs officers who are law enforcement officers

This regulation provides that customs officers who meet certain criteria are law enforcement officers for the purpose of the Act.

Parts 9, 10, 11 and 12 Reporting maritime transport security incidents, Information-gathering, Enforcement and Review of decisions

The text under each of these headings is a note indicating that this Division heading is reserved for future use. These Divisions will be inserted in the second tranche of regulations.

Part 13 Miscellaneous

13.05 Ship security alert systems

This regulation specifies that certain types of Australian ships must have a ship security alert system. It also specifies the timeframe in which the ship security alert system must be established.

This regulation also provides certain functional requirements of a ship security alert system. The requirements of this regulation are based on regulation 6 of Chapter XI-2 of the SOLAS Convention.

Regulation Impact Statement

Please note that this Regulation Impact Statement (RIS) was prepared for the introduction of the Maritime Transport Security Bill 2003 into Parliament. This RIS is being re-tabled because it was not necessary to prepare a separate RIS for the Maritime Transport Security Regulations 2003. The RIS for the Bill covers the regulatory impact of the regulations.

Part 1 Problem

The terrorist attacks since 11 September 2001, the attack on the French tanker *Limburg,* and the Bali bombing have raised global awareness and concern of the devastating effects terrorist attacks can have on human life, public infrastructure, and private industry assets and operations. At the international level and in many cases at the national level there has been a realisation that public and private assets, critical infrastructure, and business operations may not be adequately protected from the risk of being the target of a terrorist attack or other equally disruptive unlawful activity.

In the case of the maritime industry, the International Maritime Organization (IMO), the principal maritime industry body at international level, addressed this problem by developing a new preventive security regime to enhance security at ports, terminals, facilities, and on board ships. The new regime has been given effect through amendments to the Safety of Life at Sea (SOLAS) Convention, 1974. The relevant amendment to SOLAS is the newly inserted Chapter XI-2 and its companion, the two-part International Ship and Port Facility (ISPS) Code. Part A of the ISPS Code is mandatory for Contracting Governments, and Part B is recommendatory. It should be emphasised that Chapter XI-2 and the ISPS Code establish a *preventive* security system with commonsense security measures and activities for operators of ports, facilities, terminals and ships to implement. It is not intended to replace any national or international counter-terrorism response mechanisms or other law enforcement activities.

Australia is a signatory to SOLAS and adopted the amendments to SOLAS at the IMO's Conference of Contracting Governments in December 2002. The deadline for implementation of Chapter XI-2 and the ISPS Code is tight. Contracting Governments will have been deemed to have accepted the amendments by the end of 2003 - unless an objection is lodged - and are required to ensure that the requirements in Chapter XI-2 and the ISPS Code have been adequately implemented by 1 July 2004. To do so, the Australian Government has deemed it appropriate to establish a regulatory system to guide the Australian maritime industry towards compliance with the international regime by 30 June 2004.

The consequences of not establishing an efficient regulatory maritime security regime to compliment the international one range from significant reduction in business operations for those Australian maritime industry participants (eg. ports, facilities, terminals, ships) who are not compliant and may therefore be excluded from trading with compliant international maritime industry participants to serious infrastructure and asset damage due to a terrorist incident which could have been prevented by implementing the preventive security arrangements contemplated in the Maritime Transport Security Bill (the Bill). The map below demonstrates the maritime security challenges Australia faces.

A report from the Organisation for Economic Co-operation and Development (OECD) from July 2003 entitled `Security in martime [sic] transport: risk factors and economic impact' indicates that world trade depends on maritime transport and that the vulnerabilities of the maritime transport sector range from the possibility of physical breaches of the integrity of shipments and ships to document fraud and illicit money-raising for terrorist groups. The stakes, the OECD report emphasises, are extremely high because any major breakdown in the maritime transport

sector would fundamentally cripple the world's economy. The United Nations Conference on Trade and Development estimates that 5.8 billion tonnes of goods were traded by sea in 2001 which accounts for 80% of world trade by volume. The bulk of trade is carried by over 46,000 vessels servicing nearly 4,000 ports throughout the world. The OECD report makes two critical conclusions:

1. the costs of inaction are potentially tremendous because the costs of government and/or industry reaction to an attack are far greater than the costs of adequately equipping a port, port facility or ship with preventive security measures; and

2. benefits will flow from enhancing security at ports, port facilities and on board ships, such as reduced delays, faster processing times, better asset control, decreased payroll due to improved information management systems, fewer losses due to theft, and decreased insurance costs.

These conclusions align with the policy position of the Australian Government and underpin the rationale for the Maritime Transport Security Bill.

Part 2 Objectives

The primary objective for the Australian Government in taking action is to adequately safeguard against unlawful interference with maritime transport in Australia. A secondary objective is to establish a national regulatory framework to assist maritime industry participants to comply with the requirements in Chapter XI-2 and the ISPS Code. This will enable the Australian Government to inform the IMO by the deadline of 1 July 2004 that Australian ports, facilities, terminals and ships are compliant with the new international rules. As a result there will be no disruption to trade with other SOLAS signatories. The Problem identified in Part 1 above will be adequately addressed through the implementation of these objectives.

When pursuing these objectives the Australian Government is not intending to impact adversely on:

- existing counter-terrorism arrangements, law enforcement legislation and police operations at the Commonwealth, State or Northern Territory level;

- other Commonwealth operations and activities at ports (such as border protection);

- the relationship between State and Northern Territory governments with ports under their jurisdiction; or

- the efficient operations of the maritime industry participants to be regulated.

Part C Options

The main options available to the Australian Government are described below.

Option 1 Explicit government regulation

To ensure that Australian maritime industry participants are compliant with the IMO maritime security regime, the Bill proposes an outcomes based maritime security framework to regulate the maritime industry. The universal application of a single regulatory system for maritime security will provide maritime industry participants throughout all States and the Northern Territory with a consistent approach and a central regulator, which is the Department of

Transport and Regional Services (DOTARS). DOTARS will assume the responsibility for and costs associated with the assessment of security plans, verification of ship security, liaison with industry, coordination of national maritime threat information, and communication with the IMO on industry compliance issues.

At the last Australian Transport Council (ATC) meeting in May 2003, State and Northern Territory Transport Ministers agreed to the National Maritime Transport Security Framework - the precursory to this Bill - as developed by the Australian Government with the stakeholders from the States, the Northern Territory and industry. The key element of the framework is to put in place preventive security measures to protect Australia's ships, ports and port facilities from the threat of terrorism in accordance with Australia's obligations as signatory to SOLAS. The Transport Ministers also expressed commitment to meeting the international deadline for compliance of 1 July 2004.

This option is considered optimal.

Option 2 Self-regulation

Self-regulation refers to the circumstances where industry formulates the rules for its own operation and where industry is solely responsible for the enforcement of these rules. An example of this would be a code of conduct developed by a peak industry body. A voluntary code would contain the requirements in Chapter XI-2 and the ISPS Code, and it would operate in a similar way to the International Standards Organization (ISO) system. Ships, ports and facilities that wished to comply with the code would seek a certificate of compliance from the organisation administering the code in Australia.

It is suggested that this option would not result in adequate implementation of the IMO security measures because there would be no legislative backing to ensure compliance by Australian flag ships, ports and facilities and therefore no need to comply. A voluntary code would create significant uncertainty as to whether ports, facilities and ships are complying with requirements to upgrade security measures to meet increased risks. In addition, a voluntary code may not satisfy the requirements of foreign ship operators and ports, in which case they may prefer not to trade with Australian ports, facilities and ships.

The general public, for example those undertaking holiday cruises or living in the vicinity of a port facility or port, are becoming increasingly sensitive to maritime security issues. Allowing industry to set security standards would not assuage increasing public concern over maritime security. A terrorist incident involving a major port near residential areas or on board an international cruise liner with Australian citizens aboard would have a major impact on the Australian community.

The potential social and economic consequences of an ineffective industry self-regulatory scheme are too great to permit industry to determine their own standards through a voluntary code of conduct on the matter of maritime transport security.

Option 3 Devolution of the responsibility for maritime security regulation to the States and Northern Territory

Under this option the Australian Government would enact legislation to set out minimum security standards, and the responsibility for regulating the industry would be devolved to the States and the Northern Territory. The legislation would also need to include obligations placed on States and Northern Territory authorities to undertake the administration of the requirements in the amendments to SOLAS and the ISPS Code. The regime would need to be agreed to by the State and Northern Territory governments. The most likely administrative model would be for the

Australian Government to enact an overarching statutory framework which would be mirrored at the State and Territory level according to jurisdictional responsibilities, administrative arrangements and local industry needs.

The two-step process of, firstly, the Australian Government enacting legislation and, secondly, each State and Northern Territory following suit would be time consuming and costly. It would be extremely unlikely for this process to be completed in enough time to ensure industry compliance with the international deadline of 1 July 2004.

Even if State and Northern Territory legislation was introduced in time for security plans to be approved and ships to be issued with International Ship Security Certificates, it is likely that each State and the Northern Territory would not have matching systems in place. This might lead to unfair advantages and confusion, particularly where foreign masters and crew have to adapt to seven different regulatory systems when visiting different State and Northern Territory ports in Australia. It would not be in Australia's best trading interests, or in the interests of Australia's maritime industry, to have seven different, locally controlled regulatory schemes.

As mentioned above, State and Territory Transport Ministers have acknowledged the need for the Australian Government to take the lead role in maritime transport security regulation.

Part 4 Impact Analysis

Due to the urgency of the task and the international compliance deadline, there has not been time to subject the regulatory model proposed in the Bill to detailed quantitative and qualitative research to determine the impact of the Bill on the Australian maritime transport industry, other jurisdictions, and consumers. Nonetheless, information gathered during the period leading up to the development of the Bill strengthens the need for the enhancement of transport security in the maritime sector and is supportive of the proposed regulatory action. The conclusions drawn from the above mentioned OECD report reinforce this view. Ultimately, the cost of enhancing security whether in the maritime transport sector, aviation transport sector, or at home, can only be measured against the benefits from preventing unlawful interference, and the adverse economic impact unlawful interference can have on commercial enterprises and the adverse psychological impact it can have on personal wellbeing.

The assessment of the options discussed below are based on quantitative research undertaken by an independent consultant employed by DOTARS in December 2002, the OECD report referred to above, and the outcome of consultations DOTARS held with industry and State and Northern Territory government stakeholders.

Option 1 Explicit government regulation

Benefits

Under the Australian Constitution, the Australian Government has the responsibility for the obligations arising from adopted and accepted international treaties. The international obligations arising from Chapter XI-2 and the ISPS Code are considerable, and the Australian Government will need to be able to report positively to the IMO on, or before, 1 July 2004 about the domestic implementation of the treaty obligations. With this in mind and despite the tight deadline, the Australian Government has prepared a Bill which provides certainty to state-regulated entities, privately operating port facilities and the Australian shipping industry, sets penalties for offences including serious penalties for trespassing, and creates a new centralised regulatory regime with DOTARS as the regulator. Universal application is critical to ensure Australia's international obligations are met on time and to a standard acceptable to all Australian jurisdictions and affected industry participants.

A direct benefit of the Bill is that it provides a nationally consistent framework for a preventive maritime security system. The consequences of non-compliance is high and ranges from detrimentally affecting relations with international trading partners to the adverse consequences of a terrorist attack on the public health and safety as well as government and private industry assets and business operations.

There are numerous indirect benefits to managing maritime security through explicit government regulation, including upholding Australia's reputation as a `secure' trading partners, centralising the cost of administration, improving waterfront occupational health and safety, and reducing maritime industry participants' insurance costs by reducing the instances of theft and property damage.

Costs

Security regulated ports, including port facilities within these ports

The Bill places obligations on port authorities and/or those entities controlling vital areas of water in ports or approaches to ports to take an active role in port security. This is necessary because the definition of a `port facility' in Chapter XI-2 and the ISPS Code refers to a *location* which covers areas where ship-port interfaces take place rather than an entity, such as a port authority or a Harbourmaster. The definition of the international term `port facility' includes areas where direct interfaces take place as well as indirect interfaces, such as anchorages, waiting berths and seaward approaches. In the Bill, security regulated ports will be those ports which interface directly or indirectly with the types of ships which are subject to the Bill.

The regulation of ports is not without jurisdictional complexities. Ports are traditionally under the jurisdiction of the States and the Northern Territory. As a result, this Bill will have cost and resource implications for the States and Northern Territory governments. At the Australian Transport Council (ATC) meeting in May 2003 it was agreed with States and Northern Territory Transport Ministers that for the purpose of implementing the international maritime security regime the Australian Government would need to be able to regulate the entities controlling waterways. The States and the Northern Territory will be obliged to provide adequate security of their assets as owners of these assets. This is in line with the Commonwealth, State and Territory governments' principles on the protection of critical infrastructure as outlined in the National Counter-Terrorism Committee's paper `Critical Infrastructure Protection in Australia'.

The following statutory obligations on operators of security regulated ports, and port facilities within these ports, are most likely to have the greatest cost impact:

- Security regulated ports, and relevant port facility operators, will be obliged to self-assess existing security arrangements. On completion of security assessments, port operators, and port facility operators, will need to prepare security plans based on existing arrangements and identify additional security measures and activities to ensure compliance with the Bill. The plans will include security measures and activities to be implemented at security level 1 (default level), security level 2 and security level 3. The security plans will need to be submitted to the Secretary of DOTARS for approval, and DOTARS will assess compliance as required.

- When undertaking security assessments, port operators, and relevant port facility operators, should identify areas within their ports, and port facilities, which may require stricter access control arrangements and may qualify for the establishment of a maritime security zone under the Bill. The location of the proposed maritime security zones must be submitted to the Secretary for consideration. Once the Secretary has established such a zone the port operator, or port facility operator, will be obliged to comply with extra statutory requirements, for example,

screening of passengers and public notification of the boundaries of a zone. This is essential to support the enforcement regime outlined in the Bill.

- The Secretary may direct a port operator and/or one or more port facility operators within a security regulated port to implement extra security measures and activities on top of those already established in the port or port facility operator's security plan at the existing security level (1, 2 or 3) when an unlawful interference with maritime transport is imminent or probable.

At this early stage of implementation, it is extremely difficult to estimate the cost of enhancing security at the approximately 70 ports which will become security regulated ports, and the up to 300 port facilities within these ports. The local security assessment might show that a port or port facility is adequately equipped to be considered compliant with the provisions in the Bill. For example, some ports and port facilities may already have security equipment, such as hand-held radios, gates, closed circuit TV (CCTV), lights, communications system, fencing and security guards. In this case, additional costs due to upgrading security to meet the new requirements will be minimal.

DOTARS is not in the position at this early stage of implementation to know exactly what security arrangements exist at each port and port facility.

The OECD report referred to in Part 1 does not provide conclusive figures for port security costs as it acknowledges that these costs will vary dramatically from port to port and will depend on what security is already in place. For example, container facilities will have security in place to reduce theft. For some types of cargo there are already extra security requirements in place, for example, for dangerous goods. Staffing costs will also vary according to local labour costs. The report concludes that the highest cost items for ports are most likely to be security officers and security guards.

Given the above caveats, the figures below must be treated with caution. They are based on an early estimate made by an independent consultant engaged by DOTARS, who undertook a desktop audit of potential security costs to 50 Australian ports based on a prescriptive regulatory model. The ports were grouped into four different risk categories, ranging from the high risk Category A to the low risk Category D. A Category A port would typically comprise a range of diverse port facilities and terminals, such as container terminals, multi-purpose terminals, passenger ship terminals, liquid bulk terminals, and tug and pilot boat facilities. These terminals and port facilities would have different security needs and requirements. The consultant estimated that a Category A port would require physical security measures (eg. fencing, patrols, CCTV, etc) and procedural measures (eg. access control, etc). Table 1 reproduces an aggregate figure for Category A ports based on the consultant's estimates.

Table 1 DOTARS cost estimates for high risk Australian ports (security level 1)

Items	**$ million**
Closed circuit TV (CCTV) to monitor access to the port or port facility	33
Communications, such as radios, data links, etc	33
Guards and patrols	33
Vehicle booking/community system for the tracking and management of vehicles access and departing from port facilities	28
Perimeter lighting	11
Perimeter fencing	11
Security briefings/security committees	3
Personnel ID system	2.6
Uninterrupted power supply	2.4

Personnel x-ray system, including bag conveyor, for passenger facilities	2
Training	1
Possible additional cargo security prior to loading containers at major ports	80
Other, including cost of security assessments and security plan development	36
Total	**276**

Lower risk ports are expected to incur significantly lower costs in meeting the requirements in the Bill. For these types of ports the initial costs have been estimated to be up to $24 million.

In summary, total set-up costs to security regulated ports, including the port facilities within these ports, could be up to $300 million with ongoing costs up to $90 million p.a.

Increasing from security level 1 to 2 could mean introducing extra security measures such as additional patrols, limiting access points, increasing searches of persons, personal effects and vehicles, denying access to visitors, and using patrol vessels to enhance waterside security. The cost of such measures could be about $5,000 per day for each port or port facility concerned. Port and port facility operations should be able to continue without significant delays at this level.

Maritime security level 3 is unlikely to be imposed on a national basis. The Secretary may declare that maritime security level 2 or 3 is in force for a port or a number of facilities or terminals if a heightened security risk to maritime transport has been identified. As the intelligence used to trigger a move to maritime security level 3 will be specific, DOTARS, in consultation with other Commonwealth agencies, such as the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP), will issue specific and targeted advice, aimed at reducing the risk associated with the specific threat. In extreme circumstances coordination and response arrangements will be progressed in accordance with the National Counter-Terrorism Plan.

The costs of augmenting security at maritime security level 3 could be considerable and could result in operations being slowed down. For example, a container terminal could lose about $100,000 per day in revenue from suspension of container ship operations. Costs at liquid bulk terminals (for example, petroleum products, gas) and dry bulk terminals (for example, coal, iron ore, grain) would be considerably less as there are less people and equipment involved in the operations of such terminals.

In addition to the higher maritime security levels, the Secretary may also issue security directions to individual ports and facilities that may be affected by a particular threat. The Secretary must not give this kind of direction unless an unlawful interference with maritime transport is imminent or probable. A security direction can be given at security level 1, 2 or 3 and will be revoked by the Secretary once intelligence information has been received that the imminent or probable threat has subsided.

There will be penalties for non-compliance with the Bill. The penalties for breaching provisions which could seriously compromise maritime security are 200 penalties units for a port or port facility operator, 100 for penalties units for a minor maritime industry participant, and 50 penalty units for any person. In monetary terms, 200 penalties units for an individual equals $22,000, and for a body corporate $110,000. Infringement notices can be issued for less serious breaches of the Bill. The maximum amount of an infringement notice may not exceed one-fifth of the maximum fine that a court could impose, ie. the above monetary fines.

Regulated Australian ships

Australian ships which are of a certain type will be considered regulated Australian ships and as such will need to comply with the requirements in the Bill. The new security arrangements in the Bill apply to all Australian passenger ships and cargo ships of 500 gross tonnage and upwards on inter-state and international voyages. The Bill also has provisions which apply to foreign ships on intra-state and inter-state voyages which are referred to as regulated foreign ships.

While SOLAS and Chapter XI-2 only apply to certain types of ships on international voyages, the Australian Government decided to extend the maritime security regime to ensure broader coverage and better security of Australian ships and ports. The external affairs power in the Constitution provided the necessary head of power for the Australian Government to extend the application of the Convention to Australian ships on inter-state voyages.

The following statutory obligations on the operators of regulated Australian ships are most likely to have the greatest cost impact:

- Operators of regulated Australian ships will be obliged to self-assess existing security arrangements for their ships. On completion of the security assessments, ship operators will need to prepare security plans based on existing arrangements and identify additional security measures and activities to ensure compliance with the Bill and to qualify for an International Ship Security Certificate (ISSC). The plans will include security measures and activities to be implemented at security level 1 (default level), security level 2 and security level 3. The security plans will need to be submitted to the Secretary of DOTARS for approval, and DOTARS will assess compliance as required. The ISSC will be issued by the Secretary once security measures have been adequately implemented on board a regulated Australian ship. This certificate ensures compliance with the ISPS Code, and it is essential that ship operators obtain ISSCs for their ships if they wish their ships to trade with ports classified as secure under the ISPS Code.

- When undertaking a security assessments, ship operators should identify areas on board their ships which may require stricter access control arrangements and may qualify for the establishment of an on board security zone under the Bill. The location of the proposed zones must be submitted to the Secretary for consideration. Once the Secretary has established such a zone the ship operator will be obliged to comply with extra statutory requirements, for example, screening of passengers and public notification of the boundaries of a zone. This is essential to support the enforcement regime outlined in the Bill.

- The Secretary may direct a ship operator to implement extra security measures and activities on top of those already established in the ship's security plan at the existing security level (1, 2 or 3) when if an unlawful interference with maritime transport is imminent or probable.

At present, there are approximately 70 Australian registered trading ships (8 on international voyages and 62 on coastal voyages) that could be engaged in international or inter-state coastal trading and would be classified as regulated Australian ships under the Bill. In addition, the Bill will also apply to mobile offshore industry units. These units will be classified as ships if able to navigate the high seas. While DOTARS has not been able to obtain an accurate figure, the number of such units which are Australian registered appears to be very small.

It should be noted that ship operators could easily switch trading ships between international, inter-state and intra-state voyages. The cost estimate below assumes that all Australian registered ships that come within the ambit of SOLAS Convention Regulation 3 could be used on international or inter-state voyages.

Table 2 DOTARS cost estimates for Australian regulated ship (security level 1)

Items	**$ million**
Security in port, such as guards, watchmen, offside patrols when required	4.55
Training	3.77
Structural modifications to secure access to on-board security zones	1.65
Equipment, including the ship security alert system	0.45
Personal identification	0.45
Admin/record keeping	0.35
Other, including cost of security assessments and security plan development	1.78
Total	**13**

On the above basis it is estimated that the initial costs for complying with the requirements in the Bill will be around $13 million. Ongoing costs have been estimated to be at around $6 million per year.

For the sake of comparison, the US Coastguard (USCG) figures for ship compliance with the ISPS Code have been reproduced here from the OECD report. The USCG requires a high standard of compliance from the shipping industry. The costings per item per ship provide a benchmark for investment costs. According to the USCG assessment, the highest costs to ship operators will be crew training, the ship security alert system, auto-intrusion alarms, and additional locks and lights on board ships to detect unlawful interference.

Table 3 US Coastguard cost estimates for ship compliance with the ISPS Code (in Australian dollars)

Items	**Initial cost**	**Ongoing cost**
	per ship over 1,000 gross tonnage	**per ship over 1,000 tonnage**
Ship security alert system	$3,070	$153
Key crew training	$7,678	$7,678
Ship security assessment	$2,457	0
Ship security plan	$614	0
Ship security officer (function to be given to Master who on average would be occupied 5 days per year in this role)	$1,045	$1,045
Ship security training and drills (1 hour 4 times per year)	$581	$581
Total	**$15,445**	**$9,457**

In addition, ships to which Chapter XI-2 applies will need to be fitted out with security equipment. Tables 4, 5 and 6 are based on US Coastguard figures for compliance with Part B of the ISPS Code, which is beyond the intention of the Bill as Part B was designed by the IMO to be recommendatory only. Australian ship operators who wish to trade with the US will need to be aware of the US maritime security laws and make the necessary arrangements.

Table 4 US Coastguard figures for security equipment for a tanker (oil, gas, chemical) required to comply with Part B of the ISPS Code (in Australian dollars)

Equipment with USCG recommended quantity	**Initial cost**	**Ongoing cost**
	per ship	**per ship**
1 hand-held metal detector	$306	$15

5 hand-held radios	$1,530	$76
10 locks	$4,590	$229
5 lights	$3,060	$153
5 auto-intrusion alarms	$3,825	$191
Total	**$13,311**	**$664**

Table 5 US Coastguard figures for security equipment for a freighter required to comply with Part B of the ISPS Code (in Australian dollars)

Equipment with USCG recommended quantityInitial costOngoing cost

	per ship	**per ship**
2 hand-held metal detectors	$612	$30
5 hand-held radios	$1,530	$76
10 locks	$4,590	$229
5 lights	$3,060	$153
5 auto-intrusion alarms	$3,825	$191
1 portable vapour detector (for explosives)	$12,240	$612
Total	**$25,857**	**$1,291**

Table 6 US Coastguard figures for security equipment for ships under 1,000 gross tonnage required to comply with Part B of the ISPS Code (in Australian dollars)

Equipment with USCG Initial costOngoing cost

recommended quantity	**per ship**	**per ship**
3 hand-held radios	$918	$15
5 locks	$2,295	$114
5 lights	$3,060	$153
2 auto-intrusion alarms	$1,530	$76
Total	**$7,803**	**$358**

Ship operators will also need to consider employing a company security officer who will have a key role in enabling communication between a ship, the company and relevant authorities. If the company is operating less than 10 ships on international voyages the USCG estimates the annual salary for this function to be US$37,500 which is AU$57,575. The training for this officer is estimated to be US$3,500 per year which is AU$5,374. The salary for a company security officer in a company operating more than 10 ships on international voyages is substantially higher. There are only 8 Australian flagged ships on international voyages so this figure has not been included in this comparison.

As for security regulated ports and the facilities within these ports, increasing from security level 1 to 2 will mean introducing extra security measures. The cost of such measures could be about $2,000 per day for each ship involved in the heightened security situation. Ship operations should be able to continue without significant delays at this level.

The costs of augmenting security at level 3 depends on the type of ship. Operators of container ships are more likely to face higher security costs at security level 3. Costs to container shipping companies could be about $30,000 for each day that a container ship is delayed. The operating costs of most bulk ships are significantly less than for container ships. However, as mentioned above, the Secretary may only impose security level 3 when a threat is imminent or probable in which case the ship operator would have a vested interest in incurring the costs of higher security to protect the asset and the crew.

As for port and port facility operators, there will be penalties for non-compliance by the ship operator, or master in certain instances. The same graduated penalty scheme as above applies.

Summary of costs to maritime industry participants

The best estimate that can be made at this stage of the set-up costs to the Australian maritime sector (ports and ships) of complying with the IMO security measures would be $313 million in the first year. It is estimated that ongoing costs will be around $96 million p.a. for ships and ports.

It is important to remember that because these expenses are being required for compliance with a significant international agreement, these costs will not just apply to the Australian maritime industry sector but to shipping and port services sectors in all countries which are signatories to the SOLAS Convention. In fact, even those countries which are not SOLAS signatories, will have a vested commercial interest in complying with the minimum security requirements in Chapter XI-2 and the ISPS Code to be able to continue their current trading arrangements with the maritime sector in SOLAS countries. The global necessity for compliance investment means that the need for Australian maritime industry participants to budget for compliance with the Bill should not have a major impact on the competitiveness of Australia's shipping and port services industry.

Table 6 Summary of aggregate cost estimates (security level 1)

Maritime industry participant	**Initial investment**	**Ongoing expenses**
	$ million	**$ million**
Security regulated ports, including port facilities within these ports	$300	$90
Regulated Australian ships	$13	$6
Total	**$313**	**$96**

For illustrative purposes, the cost impact on cargo could represent about $2 per tonne on containerised cargo and 40 cents per tonne on bulk cargo. While shipping companies and port facility operators can be expected to recover the costs of security measures through their normal charging mechanisms, the final cost impact on consumers of goods carried by sea is expected to be very small.

The above costs relate to security measures and activities at security level 1. The costs would increase proportionate to the additional measures or activities to be undertaken at security levels 2 and 3. Additional costs would be incurred when the Secretary issues security directions, which can happen at security level 1, 2 or 3. Additional costs would be greatest if the Secretary issued a security direction to a maritime industry participant who was already operating at security level 3. However, in this case the probability of the terrorist incident or other unlawful interference occurring would be so high that the maritime industry participant would have a vested interest in incurring additional costs to protect his or her assets, staff and business operations from the attack or other serious damage.

It should be noted that these costs must be seen in an operational context. Firstly, the set-up costs associated with raising standards in order to meet the new security requirements will largely be capital in nature. Although purchased in Year 1, the capital assets purchased will have an effective life which is much greater. In some cases, the effective life of an asset may be 20 years. These costs would typically be represented over this 20-year period under an accrual accounting system - not on a cash basis. Secondly, the costs which are incurred through the

implementation of the security measures, although principally required for security reasons, are expected to also provide business benefits. Examples include reduced criminal activity and efficiencies from improved procedures.

A difficulty in quantifying the `costs' to industry is that the real costs are difficult to determine. Some of the costs mentioned above are in addition to the costs which would otherwise be expended through the normal course of doing business. Introducing the new security measures will effectively bring many costs forward, when infrastructure may have actually been upgraded on replacement in any event. Additionally, whilst costs are easier to quantify - at least in `book' terms - the benefits resulting from the costs are much more difficult to quantify, and may not be immediately apparent. Reduced criminal activity and improving the integrity of cargo and confidence in the business all have commercial merit and inherent value. Some of these benefits will accrue over time and are not possible to include in an informed cost/benefit analysis at this time.

It is implicit in the OECD report that lax security at ports, facilities and on board ships will be perceived to be less attractive to trading partners which strengthens the argument that compliance with the new security measures is a cost of doing business in the maritime sector.

How to meet the costs

It is the Australian Government's view that preventive security is a cost of doing business. Maritime industry participants are in a position to recover the costs of additional security measures through existing cost recovery mechanisms. The Bill does make provision for the sharing of security arrangements. This opens up the option of local arrangements between the public and private sector to assist the development of viable cost-effective approaches to maritime security. Once again, it needs to be emphasised that the cost of security at an individual port, port facility, terminal, ship, or other maritime industry service provider will depend on existing security arrangements.

In some cases, upgrading security could result in reduced insurance premiums through a reduction in the perceived level of risk. The shipping industry is already imposing surcharges arising from increased insurance premiums on ships trading to a number of countries in the Middle-East. These surcharges have ranged from $50 per container to about $290 per container for ships calling at Yemen where the terrorist attack on the French tanker *Limburg* occurred.

The costs of additional security at ports will need to be borne by State and the Northern Territory governments and the private sector. This is in line with the existing arrangements which recognise that while the Australian Government's role is to, among others, provide coordination and national leadership in areas of joint responsibility such as maritime transport, the owners and operators of critical infrastructure have the responsibility of providing adequate security of their assets. In this case, the Bill provides a system for assessing the security at State and Territory owned ports and privately owned or leased maritime facilities, and based on these assessment further investments may be necessary to ensure national compliance, consistency and fairness across all jurisdictions and ports.

In addition to potential costs for upgrading security at ports, States and the Northern Territory governments and the private sector will also need to consider the costs of enforcement. The new trespassing penalties may result in an increase in requests for police presence at ports and waterside police patrols.

Government costs

DOTARS' regulatory roles and responsibilities will include:

- assessment of port, port facility and ship security plans;
- verification of ship security and issuing of International Ship Security Certificates;
- checking of compliance;
- management of sensitive security threat information;
- negotiating agreement on Memoranda of Understanding with other Australian Government departments which will be assisting with the ISPS compliance checking of foreign ships;
- establishment of communications network with maritime industry participants;
- regular liaison with other Commonwealth departments and State and Northern Territory authorities;

undertaking of compliance checking of foreign ships and control functions regarding non-compliant foreign ships;

- regular reporting on compliance issues to the IMO; and
- staff training.

The 2003-4 budget allocation is $15.6 million over 2 years for DOTARS' administrative, compliance and monitoring duties.

Option 2 Self-regulation

Benefits

The voluntary nature of self-regulation means that maritime transport security initiatives would be implemented at the discretion of industry. There would be a fair amount of freedom and flexibility for industry to decide on how to implement the obligations under Chapter XI-2 and the ISPS Code through a code of conduct. Industry would retain ownership of the problem and the solution.

Self-regulation by industry may result in the implementation of security measures which minimise costs to industry participants and reduce need for major investment in security treatments. Industry may benefit from reduced compliance costs in comparison to explicit government regulation.

The lack of government involvement would mean that public resources would be allocated to other portfolios.

Costs

There would be administrative costs associated with the development of the code and the consultation period with key industry groups. It would be administratively advisable to establish a peak regulatory body to administer the code. There would be costs involved with the administration of this national body and its subsidiaries, if any, in all States and the Northern Territory. These costs would be passed on to code members and would add to their costs of doing business. Annual conferences and seminars would need to be held to update members on

new approaches and amendments to the code. Event hosting and travelling to events are costly, and would need to be subsidised by the members.

In return, the discretionary self-regulatory scheme may provide cost savings to members in the form of lenient security standards. There would be little incentive to comply as there will be no strict compliance and enforcement provisions in a voluntary industry code of conduct, apart from, for example, excluding members from the code or providing commercial disincentives or fines.

Non-compliance with the standards set in the ISPS Code would seriously disadvantage the reputation of Australia as a secure trading nation. To ensure a nationally consistent approach and be able to justify this approach and the impeccability of its implementation to the IMO the Australian Government would need to allocate resources to setting up a body to monitor the compliance with the code or determine a governance structure with strict terms of reference to temper industry's discretionary decision making powers regarding maritime security.

In the end, the seriousness of the problem identified in Part 1 of this RIS, and the international obligations which flow from Chapter XI-2 and the ISPS Code do not lend themselves to industry self-regulation.

Option 3 Devolution of the responsibility for maritime security regulation to the States and Northern Territory

Benefits

A benefit that would result from this approach is that the administrative costs for the implementation of Chapter XI-2 and the ISPS Code are transferred from the Australian Government to the States and Northern Territory governments. This would result in a freeing up of Commonwealth resources for other portfolios' responsibilities.

Having local knowledge of an issue and being able to determine local solutions to local problems can have positive effects on all involved. Local industry would benefit from being able to come to cooperative arrangements with their State or Northern Territory Government and associated maritime and/or transport authority. Local enforcement arrangements would be made to accommodate all budgets and human resource capabilities.

In addition, the Australian Government would not need to introduce a major piece of legislation as is being proposed here. Instead, and for the purposes of regulating how State and Northern Territory governments implement the international requirements, the Australian Government could introduce an overarching statutory framework which would enable the devolution of authority on maritime security to the other jurisdictions and result in State and Northern Territory legislation being developed. The Commonwealth framework would need to include strict reporting mechanisms because the Australian Government, as the signatory to SOLAS, would retain the responsibility of communication on industry compliance with Chapter XI-2 and the ISPS Code to the IMO.

Costs

Having seven authorities - one in each State and Northern Territory - with responsibility for implementing the IMO security measures is likely to cost significantly more than having a central authority. There could be problems with the consistency of enforcement of the security standards and this could impact adversely on Australia's export trades, particularly if other signatories to SOLAS believes that the Australian arrangements were not applied according to the international agreement across all Australian jurisdictions. The aggregate costs to business

are therefore likely to be higher not only due to administrative duplication, but also through inconsistency of application. These costs would be greatly magnified if Australia's reputation as a secure trading partner were undermined.

The Australian Government would need to maintain and resource an administrative function in order to report back to the IMO on the implementation of Chapter XI-2 and the ISPS Code.

Part 5 Consultation

DOTARS has consulted extensively with representatives from the maritime industry, Commonwealth departments, and State and Northern Territory governments and relevant authorities. Attachment 1 lists the groups of stakeholders consulted and types of forums used for consultation and information dissemination. Overall, there has been a high level of cooperation from all concerned. At State and Northern Territory level it was acknowledged at the Australian Transport Council (ATC) meeting in May 2003 that the Australian Government needed to take the lead role in maritime security regulation.

The most significant consultation process was the recent release of the exposure draft of the Bill to peak maritime industry organisations, State and Territory transport and maritime authorities, and a number of other influential organisations and senior staff. Around 40 submissions were received by the deadline. Key issues identified were:

- differences in the use of terminology between Chapter XI-2 and the Bill;
- lack of detail in the Bill;
- overlap with maritime safety issues, particularly in the definition of unlawful interference with maritime operations;
- enforcement of waterside issues;
- zoning provisions too top down;
- relationship between a port security plan and a port facility security plan unclear;
- definition of a security regulated ship difficult to understand;
- definition of critical installation unclear;
- demerit points system questioned;
- implications for existing cost recovery mechanisms at State and Territory level for port services mentioned;
- penalties on non-compliant foreign ships considered too lenient; and
- some concerns about the responsibilities attached to incident reporting.

DOTARS considered the merits of these issues and where reasonable have reflected these in the Bill. In some cases, further clarification of the intention of a particular provision, or group of provisions, in the Bill has been provided in the Explanatory Memorandum. Many of the issues raised will be addressed in the regulations as they relate predominantly to operational matters.

Part 6 Recommended Option

It is recommended that Option 1 be adopted.

ATTACHMENT A

Consultation on exposure draft

Exposure draft was sent to all key Commonwealth departments with a presence at ports, otherwise involved in the maritime industry, or with an interest in law enforcement and legal matters. The draft was also sent to peak industry bodies, State and Northern Territory premier departments and transport agencies and other relevant authorities, police agencies in all States and the Northern Territory, the Australian Local Government Association, and a number of maritime unions.

During the consultation period bilateral discussions were held with relevant Commonwealth departments and agencies, the NSW government, peak industry bodies, and the Maritime Union of Australia.

Maritime Security Working Group (MSWG)

The primary vehicle for consultation relating to the IMO's security framework is the Maritime Security Working Group. Membership comprises senior representatives of relevant Commonwealth departments, State and Northern Territory maritime and transport agencies, and peak industry bodies. The MSWG met 5 times in 2002.

Australian Transport Council (ATC)

The Australian Transport Council (ATC) is a Ministerial forum for Commonwealth, State and Territory consultations and provides advice to governments on the coordination and integration of all transport policy issues at a national level. The new maritime security measures were presented to ATC at meetings, most recently in May 2003.

Standing Committee on Transport (SCOT)

ATC is supported by the Standing Committee on Transport (SCOT) comprising a nominee of each ATC Minister, generally at Head of Department/Agency level. Maritime security issues were presented to SCOT at 3 meetings in 2002 and 1 meeting in 2003.

Australian Maritime Group (AMG)

The Australian Maritime Group is a sub-committee of SCOT. It brings together senior Commonwealth, State and Territory officials for consultations on the maritime sector. AMG discussed maritime security issues at 3 meetings in 2002 and 2 meetings in 2003.

The AMG has an ad hoc group on maritime security which met 3 times in 2002 and 5 times in 2003. The ad hoc group has closely scrutinised the policy and implementation model developed by DOTARS from the perspective of State and Territory governments with constitutional responsibility for ports, and as the owners and operators of ports and port facilities in several jurisdictions.

Industry meetings

Briefings and general presentations were provided to a range of key industry stakeholders, often at the invitation of the stakeholder organisation or group. Industry groups have included port authorities/port owners, shipping companies, State Counter-Terrorism Units, law enforcement

organisations, and peak industry associations. There were 6 meetings in December 2002 and over 40 meetings in 2003.

Preventive Maritime Security Workshops

From May to July 2003 DOTARS held preventive maritime security workshops in each State and the Northern Territory to inform industry and other interested persons about the broad approach taken in the Bill to maritime security.