REGULATION IMPACT STATEMENT

OBLIGATIONS ON AUSTRALIA AS A RESULT OF PROPOSED TREATY ACTION REGARDING AMENDMENTS TO THE ANNEX TO THE INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA (SOLAS) 1974:

CHAPTER XI-2 'SPECIAL MEASURES TO ENHANCE MARITIME SECURITY' INCLUDING THE INTERNATIONAL SHIP AND PORT FACILITY SECURITY (ISPS) CODE

Treaty tabling date: 14 May 2003

BACKGROUND

Obligations

The newly inserted Chapter XI-2 to the International Convention for the Safety of Life at Sea (SOLAS), 1974, sets out special measures to enhance maritime security. This includes obligations on Contracting Governments. Contracting Governments must set security levels and provide information to affected ships and port facilities (Regulation 3). They must establish a point of contact for ships to receive security related information from and to report their security concerns to (Regulation 7). With regard to foreign ships entering ports or wishing to enter ports, the new security regime allows Contracting Governments to exercise control measures over a foreign ship if there is reason to believe that the ship is non-compliant with Chapter XI-2 and Part A of the ISPS Code (Regulation 9). Control measures include detention or expulsion of a ship. Contracting Governments are obliged to submit security-related information to the IMO (Regulation 13).

Under Chapter XI-2, operators of certain types of ships on international voyages and mobile offshore drilling units must comply with the relevant requirements in Chapter XI-2 and Part A of the ISPS Code (Regulation 4). Ships must comply with the security levels set by a Contracting Government prior to entering a port or whilst in a port. If compliance is not possible, a ship must inform the relevant authorities prior to conducting a ship/port interface or entering a port. A ship's master shall have on board at all times information about crew recruitment and if applicable details about the charterer (Regulation 5). A ship to which the new security measures apply must have a security alert system on board (Regulation 6). Ship operators are to ensure that the ship's master has the authority of decision making with regard to the ship's safety and security (Regulation 8).

In addition to ship operators, operators of port facilities which service ships subject to the new security regime are required to comply with the relevant requirements in Chapter XI-2 and Part A of the ISPS Code, and Contracting Governments are to ensure that port facility security assessments and port facility security plans are developed, reviewed, approved and implemented (Regulation 10).

Guidelines for the implementation of the security measures are in the two-part ISPS Code. Part A of the ISPS Code sets out mandatory requirements, including responsibilities of Contracting Governments and maritime industry participants, designation of security officers, verification of ship security, issuing of International Ship Security Certificates to verified ships, cooperative arrangements, record keeping, training requirements, efficient collection of security related information (such as through a Declaration of Security), and a methodology for security assessments and the development of security plans. Part B has recommendations which refine and further clarify Chapter XI-2 and Part A of the ISPS Code.

Attachment A reproduces the segments of the ISPS Code which deal with ship and port facility security plans.

Implementation

The Government has agreed that the Department of Transport and Regional Services (DOTARS) prepare drafting instructions for the Commonwealth Maritime Transport Security Bill 2003 to implement the new maritime security measures in Chapter XI-2 and the ISPS Code. The Bill is expected to be introduced into Parliament in the 2003 Winter Sittings.

It is proposed that the Commonwealth Maritime Transport Security Bill 2003 extend the application of the new security arrangements to Australian flagged passenger ships and cargo ships of 500 gross tonnage and upwards on inter-state voyages and those port facilities serving these ships as well as oblige port authorities to take an active role in port security. The extension of security measures has been agreed to by State and Territory maritime transport authorities.

Attachment B outlines roles and responsibilities under the proposed domestic maritime security regulatory model.

A PROBLEM

Events since 11 September 2001, the attack on the French tanker Limburg and the Bali bombing indicate that there is an urgent need to re-appraise the adequacy of preventive security measures by industry, including the maritime industry. If Australia does not implement the IMO security measures, Australian ports and cities will be further exposed to the risk of a terrorist incident, as other ports around the world tighten their own security.

Failure to accept the IMO maritime security measures could seriously disadvantage Australia's trading interests, particularly to the USA. This is because international shipping companies may be reluctant to put their ships into ports that have not implemented the security measures for fear of being subject to delays at ports which have implemented the measures. Overseas ports that have implemented the measures may delay or refuse entry to ships coming from ports that do not comply with the measures.

The value of Australia's export trades carried by sea is around $100 billion p.a., with the value of exports to the USA being around $9 billion p.a.

Industry players have recognised the change in circumstances and some port authorities and shipping lines are already reviewing their current security arrangements with a view to determining what additional security measures are required. The maritime sector in Australia is awaiting guidance and guidelines from DOTARS relevant to preparing and implementing security plans to meet the IMO requirements. DOTARS is currently working on these guidelines and will be consulting the maritime sector on this matter.

B OBJECTIVE

The objective of the IMO maritime security measures is to establish a standardised international framework through which ships and port facilities can co-operate to detect and deter acts of terrorism in the maritime sector.

C OPTIONS

The main options available to the Government are described below.

Option 1: Accept the new security measures under Chapter XI-2 of SOLAS and the ISPS Code and implement through Commonwealth legislation

Acceptance of the new security measures under the Chapter XI-2 and the ISPS Code will require new Commonwealth legislation. The Government has agreed that the Department of Transport and Regional Services (DOTARS) prepare drafting instructions for the Commonwealth Maritime Transport Security Bill 2003 to implement the new maritime security measures in Chapter XI-2 and the ISPS Code. The Bill is expected to be introduced into Parliament in the 2003 Winter Sittings.

Option 2: Implement the IMO maritime security measures under a voluntary code of practice (without legislation)

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 and port facilities that wished to comply with the code would seek a certificate of compliance from the organisation administering the code in Australia.

Option 3: Not accept the IMO maritime security measures

A decision for Australia not to accept the IMO security measures could be achieved by Australia lodging an objection to the amendments within the timeframe allowed under the tacit approval procedure (by 31 December 2003).

Option 4: Devolve responsibility to the States and the Northern Territory

It is envisaged that under this option the Commonwealth would enact the required legislation and set the required security standards, but responsibility for administering the arrangements would be devolved to the States and the Northern Territory.

D IMPACT ANALYSIS

Option 1: Accept the new security measures under Chapter XI-2 of SOLAS and the ISPS Code and implement through Commonwealth legislation

Benefits

By accepting the IMO security measures, Australia would become party to an internationally agreed system for detecting and, as far as practicable, deterring terrorist activities directed against

ships and port facilities. The system would assist in preventing the maritime transport sector from being used as a means of transporting terrorists and their equipment (eg. explosives, weapons) to target areas.

Costs

Ports and port facility operators

The Maritime Transport Security Bill 2003 will apply to approximately 70 ports in Australia and around 300 port facilities. In recognition of the different roles and responsibilities of port authorities/owners and port facility operators, a method has been devised to assign a classification to ports (High, Medium and Low) and risk categories to port facilities (A, B and C, with A being the highest risk category). Criteria for determining the risk category of a port facility will include factors such as number of passengers and passenger ships handled by the facility, a critical infrastructure test, proximity to population centres, and likely economic impact of disruption to the facility in the case of a terrorist attack. The designation of a classification to a port and a risk category to a port facility will in turn determine the outcomes based security measures that ports and port facilities will need to consider when developing their security plan.

DOTARS is proposing a non-prescriptive regulatory model. Appropriate outcomes based security arrangements will be reflected in the Maritime Transport Security Bill 2003. This recognises that a prescriptive 'one size fits all' approach would impost on the maritime industry and potentially be more costly than necessary to achieve the desired aim. Local level security assessments will identify risks that need to be treated at the port, port facility and ship level, and security measures appropriate to treat these risks will be identified by the operator themselves and addressed in their security plans.

Information obtained from port authorities and operators of port facilities indicates that terminals facing relatively higher risks of terrorist activity, such as cruise liner terminals and oil or petroleum products terminals, already have security measures in place. In a number of cases these measures are in the process of being reviewed and upgraded. It is expected that upgrading or installing new security measures at port facilities will include ensuring that the new security standards are met.

Given the proposed regulatory model, costs to port facility operators and ports will vary. They will depend on existing arrangements and the outcome of a security assessment. The figures listed below are based on an initial estimate made by an independent consultant engaged by DOTARS.

Indicative breakdown of costs for Category A port facilities:

Item	**$ million**
Closed circuit TV to monitor access to the facility	33
Communications, such as radio, 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 terminals	2
Training	1
Possible additional cargo security prior to loading containers at major ports	80
Other, including cost of security assessments	36
TOTAL	**276**

A major container handling facility may wish to install the latest technology for cargo screening, such as a gamma ray machine. Others may prefer to employ more security staff and/or accept electronic seals on containers. The cost of screening cruise ship passengers will be unique to cruise ship terminals.

Lower risk port facilities, such as wharves and terminals handling dry bulk cargoes and general cargoes, are expected to incur significantly lower costs in meeting the new security requirements. For these port facilities the set-up costs have been estimated to be up to $24 million.

In summary, total set-up costs to port facilities and ports could be up to $300 million with ongoing costs up to $90 million p.a.

Shipping

The main additional costs to owners of Australian flagged ships to which the proposed Maritime Transport Security Bill 2003 will apply will be the securing of critical areas of a ship's operations (eg. navigating bridge and engine room), having a ship security alert system on board, complying with security in ports and at port facilities, and managing new administrative and procedural requirements, such as preparing ship security plans, appointing and training persons to perform the functions of a company security officer and ship security officer, and record keeping.

At present there are approximately 70 Australian flagged 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 subject to the proposed Maritime Transport Security Bill (ie. all passenger ships on inter-state and international voyages, and international and inter-state trading and cargo ships of 500 gross tonnage and upwards on international voyages). In addition to certain types of cargo

and passenger ships, the IMO security measures also apply to mobile offshore drilling units (MODUs). There are no Australian flagged MODUs.

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

Indicative breakdown of the set-up costs:

Item	**$ million**
Security in port, such as guards, watchmen, offside patrols when required	4.55
Training	3.77
Structural modifications to secure access to the bridge, engine room and other restricted areas	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 certification	1.78
TOTAL	**13**

On the above basis it is estimated that the set-up costs of applying the new security measures to Australian flagged ships would be around $13 million in the first year. Ongoing costs in subsequent years have been estimated at around $6 million p.a. These estimates are broadly in line with estimates made in the United States.

Cost of increasing security levels

The normal operating environment will be security level 1. Port, port facility and ship security plans will need to outline the minimum protective and additional security measures that will be maintained at levels 1 and 2. It will also be a requirement for plans to outline the proposed additional security measures if advised of a move to security level 3. DOTARS reserves the to right to determine additional security measures at its discretion in light of specific advice on national security.

Security level 3 is unlikely to be imposed on a national basis. Rather, it will be a level reserved for preparing for specific threats based on credible advice that an incident is imminent. As the intelligence used to trigger a move to security level 3 will be specific, DOTARS, in consultation with other Commonwealth agencies (ie. intelligence services, Federal Police, etc) 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.

With regard to the costs, increasing to security level 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 facility concerned, and about $2,000 per day for each ship involved in the heightened security situation. However, it is

anticipated that at security level 2, ship and port facility operations should be able to continue without significant delays.

The costs of implementing security level 3 measures could be considerable. For example, as a worse case, a container port facility could lose about $100,000 per day in revenue from suspension of container ship operations, and the cost to shipping companies could be about $30,000 for each day that a container ship is delayed. Costs at liquid bulk facilities (eg. petroleum products, gas) and dry bulk facilities (eg. coal, iron ore, grain) would be considerably less as there are less people and equipment involved in the operations of such facilities. The operating costs of most bulk ships are significantly less than for container ships.

Summary of costs to Australian maritime sector

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.

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 the base level security measures (ie. security level 1). Costs would increase to the extent that measures under security level 2 and 3 need to be imposed as a result of increased levels of threats of terrorist attacks in the maritime sector.

More accurate figures on the cost to the Australian maritime sector of meeting the obligations under the IMO security measures will not be known until the ship and port facility security assessments have been carried out, and the security measures appropriate to the assessed level of risk have been determined.

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 will be 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 shrinkage, criminal activity, integrity of cargo and confidence in the business (eg. goodwill) are all not without commercial value. However, these benefits will accrue over time and are not possible to include in an informed cost/benefit analysis at this time. The true real cost to business is difficult to determine. Above all, the commercial operating environment is increasingly of the view that lax security at port facilities is perceived as less attractive to business partners, further strengthening the argument that compliance with the new security measures is a cost of doing business in the maritime sector.

How should costs be met

The Government's approach in the transport sector is that preventive security is a cost of doing business and should be met by the industry parties concerned. As mentioned earlier, the maritime sector is in a position to recover the costs of additional security measures through existing user-pays charging mechanisms.

It should be noted that 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 – this is the result of the terrorist attack on the French tanker 'Limburg' as it approached a port in Yemen).

DOTARS costs

DOTARS will incur significant costs as DOTARS' regulatory roles and responsibilities will range from, among others, development of a new maritime industry security program for 70 Australian flagged ships, 70 ports and approximately 300 port facilities, efficient administration of this program, verification of ship security and issuing of International Ship Security Certificates, auditing of compliance with the security program, and regular reporting on compliance issues to the IMO. Attachment B summarises DOTARS' roles and responsibilities.

Option 2: Implement the IMO maritime security measures under a voluntary code of practice (without legislation)

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 and port facilities. In particular, a voluntary code would create significant uncertainty as to whether ships and port facilities would comply with requirements to upgrade security measures to meet increased risks.

Furthermore, Australia would not be able to enforce the IMO security control measures to restrict or prohibit the entry of foreign ships to Australian ports, where such ships do not comply with the IMO security measures and there are clear grounds for believing that the ship poses a security risk.

For the above reasons Option 2 is not considered acceptable as a long term arrangement.

Option 3: Not accept the IMO maritime security measures

Benefits

The Australian shipping and port industries, and government agencies responsible for maritime matters would be spared the cost of implementing the IMO security measures.

Costs

Non-acceptance of the international maritime security measures would leave Australia without adequate preventive measures to deal with terrorist and related unlawful acts against its ports, international cargo and passenger ships using those ports. Ships carrying Australian exports to countries that have accepted the IMO security measures (particularly the USA) could be subject to serious delays and possible refusal of port entry.

It is not possible to assess the cost of non-acceptance of the IMO security measures, but such costs could far exceed the costs of accepting and implementing the measures. The possibility of ships carrying exports from Australian ports that do not comply with the IMO security measures being held up in foreign ports (especially the USA) could result in the permanent loss of valuable export markets and major disruption to Australia's other international trading interests.

The value of Australia's export trades carried by sea is around $100 billion p.a., with the value of exports to the USA being around $9 billion p.a.

Option 4: Devolve administrative responsibility for maritime security to the States and the Northern Territory

As we are dealing with an international treaty, the Commonwealth has the responsibility of the 'Contracting Government' under the provisions of the new SOLAS Chapter XI-2 and the ISPS Code. Under these provisions the Commonwealth Government could appoint an authority in each State and the Northern Territory to administer security arrangements applying to ships and port facilities.

As regards legislation, the most appropriate arrangement may be for the Commonwealth to enact the required legislation and set the required standards. The legislation would also need to include obligations placed on States and Northern Territory authorities to undertake the administration of the IMO maritime security arrangements. The regime would need to be agreed by the State and Northern Territory governments. The most likely administrative model would be for the Commonwealth to enact model legislation and for the States and Northern Territory to enact mirror legislation.

The process of each State and Northern Territory enacting its own legislation (mirroring the Commonwealth legislation) in order to implement the IMO security measures would be very time consuming, and would be unlikely to be completed in time for Australia to implement the measures within the required timeframe (legislation passed by December 2003 and full compliance by July 2004).

Benefits

From a national perspective there do not appear to be any benefits under this option. All that could be achieved is a transfer of administrative costs from DOTARS to State/Northern Territory authorities.

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 one authority within DOTARS. There could also be problems with inconsistencies in the enforcement of security standards and this could impact adversely on Australia's export trades, particularly to the USA if that country were to determine that the Australian arrangements were not applied to an appropriate standard. 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.

Additionally, the Commonwealth would still need to maintain an administrative function in order to report back to the IMO, and to provide some measure of assurance that States/Northern Territory were implementing Chapter XI-2 and the ISPS Code appropriately. Costs would be significantly higher, not only because the States/Northern Territory would recreate the administrative function, but also because the Commonwealth's administrative function would not be able to be totally replaced.

Hence, a single regulator, that is, Option 1, will provide the business community with a single response to Chapter XI-2 and the ISPS Code. This will provide an improved basis for planning and infrastructure purchasing decisions, which provides for increased confidence to make investment decisions; ultimately this provides for increased efficiency within the Australian maritime sector to the benefit of Australia as a whole.

E CONSULTATION

DOTARS has been consulting extensively with representatives from the maritime industry, and relevant Commonwealth, State/Northern Territory authorities. In this regard the Government agreed early in 2002 that DOTARS establish a high level Commonwealth/State/Industry working party – the Maritime Security Working Group (MSWG). DOTARS has also been consulting regularly with the States and Northern Territory governments through the Australian Maritime Group (AMG) which forms part of the Australian Transport Council (comprising Commonwealth and State/Northern Territory Ministers responsible for transport matters).

To date there has been a high level of cooperation from all concerned, and the maritime industry has accepted the need for additional security measures provided these are commensurate with the assessed risks. However, as noted above risk assessments are still to be undertaken and the security standards to be complied with by industry have not been completed. DOTARS will continue to consult with all relevant parties with a view to achieving a consensus on the standards to be applied.

F RECOMMENDED OPTION

It is recommended that Option 1 be adopted.

ATTACHMENT A

OBLIGATIONS UNDER THE ISPS CODE: SHIP AND PORT FACILITY SECURITY PLANS

Content of Ship Security Plans (ISPS Code, Part A, Section 9.4)

.1 measures designed to prevent weapons, dangerous substances and devices intended for use against people, ships or ports and the carriage of which is not authorised from being taken on board the ship;
.2 identification of the restricted areas and measures for the prevention of unauthorised access to them;
.3 measures for the prevention of unauthorized access to the ship;
.4 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;
.5 procedures for responding to any security instructions Contracting Governments may give at security level 3;
.6 procedures for evacuation in case of security threats of breaches of security;
.7 duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;
.8 procedures for auditing the security activities;
.9 procedures for training, drills and exercises associated with the plan;
.10 procedures for interfacing with port facilities security activities;
.11 procedures for the periodic review of the plan and for updating;
.12 procedures for reporting security incidents;
.13 identification of the ship security officer;
.14 identification of the company security officer including with 24-hour contact details;
.15 procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;
.16 frequency for testing or calibration any security equipment provided on board;
.17 identification of the locations where the ship security alert system activation points are provided;[1] and
.18 procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.[1]

Content of Port Facility Security Plans (ISPS Code, Part A, Section 16.3)

.1 measures designed to prevent weapons or any other dangerous substances and devices intended for use against people, ships or ports and the carriage of which is not authorised, from being introduced into the port facilities or on board a ship;
.2 measures designed to prevent unauthorised access to the port facility, to ships moored at the facility, and to restricted areas of the facility;

[1] Administrations may allow, in order to avoid any compromising of the objective of providing on board the ship security alert system, this information to be kept elsewhere on board in a document known to the master, the ship security officer and other senior shipboard personnel as may be decided by the Company.

.3 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface;
.4 procedures for responding to any security instructions the Contracting Government, in whose territory the port facility is located, may give at security level 3;
.5 procedures for evacuation in case of security threats or breaches of security;
.6 duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects;
.7 procedures for interfacing with ship security activities;
.8 procedures for the periodic review of the plan and updating;
.9 procedures for reporting security incidents
.10 identification of the port facility security officer including 24-hour contact details;
.11 measures to ensure the security of the information contained in the plan;
.12 measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility;
.13 procedures for auditing the port facility security plan;
.14 procedures for responding in case the ship security alert system of a ship at the port facility has been activated; and
.15 procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers' welfare and labour organizations.

ATTACHMENT B

PROPOSED ROLES AND RESPONSIBILITIES UNDER THE MARITIME TRANSPORT SECURITY BILL 2003

Port authorities and port facilities

To ensure that Australia has a comprehensive port security regime that addresses both our domestic security requirements and our international obligations, both port facilities and port authorities will be included in Australia's maritime security arrangements. *Port authorities* will be responsible for port wide security matters. While the SOLAS amendments focus on *port facilities*, in many cases, port authorities, corporations or administrators already fulfil or must take on a security role with regard to areas and facilities integral to ports, such as the waterside, pilots, tugs and common user berths.

Port authorities will be required to:

- establish Port Security Committees, which will meet regularly, oversee the conduct of a Port Security Assessment consistent with risk management standard AS/NZ 4360:1999, and develop a Port Security Plan;
- submit the Port Security Plan with the Port Security Assessment to DOTARS for approval;
- once approved, delegate the Port Security Committee to implement and monitor the security measures as per the Plan and according to DOTARS' port classification, including use of the harbour control systems for security outcomes;
- appoint a Port Security Officer;
- ensure the Plan is exercised and submitted to testing, monitoring and evaluation;
- act promptly on directions given by DOTARS about changes in security levels and requirements for additional security measures.

Similarly, individual *port facilities* in ports will be required to:

- conduct a Port Facility Security Assessment consistent with risk management standard AS/NZ 4360:1999 for the facility, then develop a Port Facility Security Plan;
- submit the Port Facility Security Plan with the Port Facility Security Assessment to DOTARS for approval;
- once approved, implement and monitor security measures as per the Plan and according to DOTARS' port facility categorisation;
- appoint a Port Facility Security Officer;
- ensure the Plan is exercised and submitted to testing, monitoring and evaluation;
- cooperate with the Port Security Committee and integrate Port Facility Security Plan with the Port Security Plan;
- provide an appropriate representative to the Port Security Committee;
- act promptly on directions given by DOTARS about changes in security levels and requirements for additional security measures.

There may be opportunities for port facilities to combine their efforts in these matters, particularly if local facilities share similar characteristics, are considered to be a low security risk, or are the

responsibility of a single entity. For example, pilots, tugs, waterside areas and common user berths in a low security port could all be treated as a single facility if all managed by the same port authority or entity. A low security coal terminal co-located with a low security wheat facility operated by the same firm could be treated as a single facility.

Ship operators

With regard to ships affected by the proposed regulatory regime, ship operators' responsibilities will be to:

- install an on board Ship Security Alert System;
- designate a Ship Security Officer for each vessel and a Company Security Officer;
- undertake Ship Security Assessments, after which Ship Security Plans must be developed and implemented;
- submit Ship Security Plans with the Security Assessments to DOTARS for approval;
- arrange for valid International Ship Security Certificates (ISSCs) to be issued by DOTARS;
- act promptly on directions given by DOTARS about changes in security levels and requirements for additional security measures.

Department of Transport and Regional Services (DOTARS)

DOTARS' role will be to:

- prepare a National Maritime Sector Risk Context Statement;
- determine national criteria for classification of ports and categorisation of port facilities;
- determine minimum outcome-based security standards;
- develop model security plans for ships, ports and port facilities;
- provide guidance material on the use of Australian/New Zealand 4360; 1999 Risk Management Standard as part of the security assessment process;
- approve or reject security plans, and if applicable, request variations to security plans;
- issue ISSCs;
- audit the implementation of standards (as per security plan) and work with industry to address non-compliance issues;
- determine the requirement for a Declaration of Security;
- inform the IMO of compliance matters as specified in Chapter XI-2/13 of SOLAS.

In addition to managing these administrative tasks, DOTARS will be responsible for these operational functions:

- communicate with ships, security officers, others (as required) of changes in security levels;
- advise ships, security officers, others (as required) of additional security measures necessary at any time;
- advise ships, security officers, others (as required) of additional security measures necessary at Security Levels 3;
- designate a 24-hour departmental point of contact for incident reporting;

- act as point of notification when a verified ship security alert has been activated and take appropriate action;
- instruct the requirement for a Declaration of Security (DOS);
- receive information on the DOS's requested and completed;
- resolve safety/security conflicts when raised by masters;
- request security related information from foreign ships and imposing control measures when necessary.

Some of these functions will affect other Commonwealth Departments and Agencies. Exercising these responsibilities may also involve or affect State and Territory Departments and Agencies.

Some of these responsibilities fall under the National Counter-Terrorism Committee arrangements, others are outlined at a port and/or facility level in their respective security plans.