

SECURITY GUIDELINES FOR FERRY AND CHARTER VESSEL OPERATORS

Table of Contents

DEFINITIONS	Page 3
INTRODUCTION	Page 4
Purpose	Page 4
Approach	Page 4
National Counter Terrorism Levels	Page 4
RECOMMENDED APPROACH TO SECURITY	Page 5
Security Management	Page 5
The Security Threat	Page 5
People and Security	Page 5
Security Outcomes for Vessel Operators	Page 6
DEVELOPING A SECURITY PLAN	Page 6
Involvement	Page 6
Steps to Better Security Outcomes	Page 6
ATTACHMENTS	
Annex A – Security measures at each threat level	Page 9
Annex B – Vessel Security Plan Template	Page 14

DEFINITIONS

Commercial Purpose A reference to the use of a vessel or motor for a commercial purpose is:

In the case of a vessel-a reference to the use of a vessel:

- (i) for the carriage of persons or goods for money or any other valuable consideration.
- (ii) in any way in, or in connection with, a business or trade or commerce.
- (iii) by hiring it out, or making it available, in the course of a business, or in trade or commerce....

(Commercial Vessels Act 1979 Sect 5)

Ferry: Means a vessel which seats more than 8 adult persons, and includes a vessel of any class prescribed by the regulations for the purpose of this definition

(Passenger Transport Act 1990 No 39)

Ferry Service: Means any ferry service for the carriage of passengers.

(Transport Administration Act 1988 No 109)

Non-Security Regulated Ships: Those commercial vessels not covered by the *Maritime Transport and Offshore Facilities Security Act 2003*.

Public Passenger Service: Means the carriage of passengers for a fare or other consideration:

By a vessel within any New South Wales Waterway

(Passenger Transport Act 1990 No 39)

Security Outcomes: What is expected to be achieved by security measures taken or proposed.

SMS: Safety Management System Guidelines for Charter Vessel Operators.

Vessel: In this Act, "vessel" includes watercraft of any description used or capable of being used as a means of transportation on water.

(Ports and Maritime Administration Act 1995 Sect 4)

INTRODUCTION

Purpose

The purpose of these guidelines is to assist ferry and charter vessel operators should they wish to develop a security plan to improve the security of their operations. It should be read in conjunction with the Safety Management System Guidelines for Vessel and Charter Vessel Operators (2004) Section 8 as amended.

Approach

This guide assists you to achieve practical *security outcomes* that will improve the security of your operations and the confidence of your staff and passengers. *Security outcomes* differ from security systems or security plans. You can inspect measure or test a security outcome and you can assess the extent to which it is being achieved. If you and your staff concentrate on outcomes, the security measures you put in place will make sense and your efforts will have a clear focus.

National Counter-Terrorism Alert Levels

The measures you take to achieve security outcomes will depend on the nature, or context of your particular operations. The national security context changes over time – sometimes it can change very rapidly. The security context of your operation could change just as rapidly. This means that you may need a plan to change your security measures quickly, without causing confusion or panic.

National Counter-Terrorism Alert Levels help you plan to change security measures as the security threat changes. There are four National Counter-Terrorism Alert Levels - *low, medium, high and extreme*.

Low	– terrorist attack is not expected
Medium	– terrorist attack could occur
High	– terrorist attack is likely
Extreme	– terrorist attack is imminent or has occurred

These levels are set by national authorities. Any change to the National Counter-Terrorism Alert Level will be communicated widely in the media. You also may receive information directly from the NSW Police. Information about National Counter-Terrorism Alert Levels can also be found here - <http://www.nationalsecurity.gov.au>. Your operation should have a process to check this site on a regular basis. Your operation will already have a range of plans and measures in place for safety, emergency and security. Countering the security threats posed by potential terrorist threats should be an extension of these existing arrangements. The security measures discussed in this guide are not exhaustive. They do not form a 'must do' list of measures. They are intended for consideration by operators responsible for security within their own organisation or sphere of operations. Your security arrangements should not be restricted to the measures outlined in this paper – you know your operation best.

Recommended Approach to Security

Good security is good business!

Security Management

Security management is a safeguard to provide a secure environment on your vessel and to reduce the opportunity and potential for intentional criminal or terrorist acts that may harm customers or staff or may reduce the effectiveness of your business.

The Security Threat

The security threat posed by terrorism is very real. Public transport may be a target for terrorism, among many other potential targets in our community. Bus, Rail, Ferry mass passenger transport systems and charter vessels concentrate large numbers of people in the confines of vehicles, ferries and at interchanges at predictable times.

The transport interfaces at major sporting and entertainment complexes are also subject to crowding at predictable times. Ferry, Charter vessel, bus and rail interchanges, particularly at the conclusion of large events, are regularly crowded for extended periods. These occasions could provide a target that offers a combination of mass casualties and symbolic impact, particularly where they involve major sporting events.

You may wish to refer to the Surface Transport Risk Context Statement as provided by the Department of Infrastructure, Transport, Regional Development and Local Government setting out the range of risk faced by public transport operators. The current statement is available at www.infrastructure.gov.au/transport/security/maritime/risk. You should read this and regularly check for updates.

People and Security

Both the *likelihood* of an attack happening and the *consequences* of a successful attack can be significantly reduced if the people who might pose a threat are identified or deterred by good security, or if their plans are interrupted by good security measures.

Security Outcomes for Vessel Operators

Security Outcomes differ from security systems or security plans. The achievement of a Security Outcome can be measured.

You can test a Security Outcome at any time – regularly check that the people working with you and your clients are the right people, that they are where they are meant to be and doing what they are meant to be doing.

Security measures, such as pre-departure and in-service vessel inspections, staff vigilance and the reporting of suspicious activity and other such measures can, and do contribute to security. You should never lose sight of why you are doing these things and what security outcomes you want these measures to deliver.

At higher levels of security alert, increase the frequency and coverage of these measures. Annex A of this set of guidelines is designed to assist you in this regard.

This approach allows you to develop effective security measures that are able to increase as the threat and consequent risks to your operations change. Once you have these arrangements in place you can also train your staff and practise changing your levels of security. Remember, the *security outcomes* you are seeking do not change – but as the threat changes, your risks increase and the measures you take will need to change accordingly.

Developing a Security Plan

Involvement

Your security plan should work for your business. Even so, there will be few, if any, cases where others are not involved in your security – at the very least it will involve the police and probably other transport operators that may use the same interchange. It is important that you communicate with these groups and operators about security, and also take into account the security risks other operations might pose to your business.

Effective security also means that you need to engage your staff and key suppliers or contractors in the process.

Planning, information gathering and communication at the outset will save time, prevent confusion and contribute to a better outcome.

Steps to better Security Outcomes

1. Get to Know your Local Police.

Your NSW Police Local Area Commander, or Marine Area Commander, can give invaluable advice to assist your security planning.

In the event of a security incident they will be your first point of contact and assistance. At times of increased threat, they may give you directions to ensure public safety. Invite a NSW Police representative to attend meetings where security matters are discussed. Ask the Police to outline their role in:

- Keeping you informed of threats to your facilities and operations;
- Crime prevention and other security advice;
- Protecting your facilities and operations; and
- Managing a crisis arising from a security incident.

2. Allocate Security responsibilities.

Allocate responsibilities for security to appropriate positions within your organisation. Owner/operators need to ensure that security issues are part of their daily planning process. Assess the security risks affecting customers, staff, vessels, vehicles, facilities and equipment (refer SMS Section 3)

3. Control Measures.

Develop control measures to eliminate or reduce identified security risks. These may include training, policies, procedures, equipment, facilities and physical resources. (Refer SMS Section 7)

4. Review Risks.

Periodically review identified security risks and the measures used to reduce or eliminate the risks (Refer SMS Section 8)

5. Report Security Incidents.

Establish procedures for staff to report security incidents and suspicious activity (Refer SMS Section 7)

6. Major Incidents.

Establish procedures to respond to major incidents and emergencies. Your risk assessment will indicate the type of hazardous events that you need to plan for. These may include events that are managed by the emergency services but may impact on your operations (Refer SMS Section 7)

7. Training.

Train your staff in security related issues including awareness, identification of risks and actions to be taken in the event of a security incident (Refer SMS Section 7)

8. Evaluation.

Evaluate and test the suitability of your security arrangements and procedures through the conduct of audits, exercises and drills (Refer SMS Section 5)

9. Liaison.

Liaise with other transport operators in relation to shared locations such as wharves or vessel interchanges that interact with other areas such as restaurants and bus/rail interchanges.

10. Increased threat levels.

Develop measures that may be implemented to respond to situations at higher threat levels and changes to the national terrorism alert levels. NSW Maritime has developed guidance material to assist in this regard (See NSW Maritime Guidelines at [ANNEX A](#) of this document)

A template for basic vessel security plan is attached at [ANNEX B](#). Security regulated ships are required to have an approved ship security plan, a template of which appears on the Dept. of Infrastructure website. Smaller charter vessel and ferry operators may choose to use the template at [ANNEX B](#) as a guide for preparing a security plan to suit their own operations. Once you have your security plan, you should ensure that employees (including contractors) are trained and able to implement basic security measures protecting your operations. You should also conduct security awareness training for staff (including contractors) and provide regular reminders of the need to follow good basic security. Training should include at least:

- The identification and assessment of security risks;
- Simple security reporting and first response (generally initial investigation and reporting to police rather than intervention);
- Emergency evacuation procedures;
- Bomb threat precautions, reporting and bomb search procedures;
- Basic First Aid skills; and
- Fixed, long standing security measures such as pre-departure vessel security inspections.

Also participate in counter-terrorism exercises as requested by Police and emergency management personnel.

Attachments: Annex A – Security Measures at Each Threat Level

Annex B – Vessel Security Plan template.

ANNEX A – SECURITY MEASURES AT EACH THREAT LEVEL

Possible Security Measures

The security measures that are right for your business will flow from the security risks you have identified during your risk assessment and security planning. The table below lists both the desired outcomes and possible security measures to consider. Several of the listed security measures may be required to achieve a single outcome. Your decisions should be based on achieving security outcomes, with security measures that can be increased in a controlled and planned manner as the threat changes.

The Table provides guidance. The outcomes and measures are provided as examples, they are not mandatory. You need to consider what mix of measures will generate the security outcomes for your business.

<u>Security Outcomes</u>	<u>Possible Security Measures</u> BLUE At LOW and MEDIUM Alert, add AMBER at HIGH Alert, and add RED at EXTREME Alert
People (always applicable)	
The right people access your operations.	Establish and maintain an effective security perimeter, with signage around your own area, eg securing of vessel prior to departure each day and after hours. (staffed at higher security alert levels).
People access your operations at the time and place they are required to.	Undertake routine security perimeter checks, report security breaches and make rapid repairs – consider physical patrolling at higher alert levels.
People access the part of your operations they are authorised to.	Control access to non public areas of your operations, such as time in and time out booking for authorised visitors arriving and leaving important facilities – consider meeting all visitors off site at higher levels of alert.
People are being escorted in your operations should they be required to.	Time in and time out booking for staff entering and leaving important facilities. Adopt visible ID for permanent staff and authorised visitors – consider visitor escort at higher levels of security alert – consider denying all visitor access at highest alert levels
People leave your operations when their authorised business or activity is completed.	Perform random ID and authorisation checks at access points and inside facilities and administration areas.
People leave at the time and place they are required to.	Perform staff checks and questioning at interviews – consider police checks for key staff. Report people acting suspiciously such as those making sketches or taking photos of transport facilities or who try
People that are meant to be in your operations are able to be readily recognised and their authorisation checked.	

<p><u>Security Outcomes</u></p>	<p><u>Possible Security Measures</u> BLUE At LOW and MEDIUM Alert, add AMBER at HIGH Alert, and add RED at EXTREME Alert</p>
<p>The people in your operations do not pose a threat.</p> <p>People who do pose a threat do not have the time required to carry out the threat.</p> <p>People have the right skills, training and personal equipment for their purpose or location.</p> <p>All the people in your operation understand and actively exercise their role in security and emergency management arrangements.</p>	<p>to evade notice when detected.</p> <p>Report people acting suspiciously such as those who loiter at transport facilities with no apparent intention of using transport services.</p> <p>Place signage in vessels to encourage passengers to identify and report suspicious behaviour, eg security checklist posters.</p> <p>Train staff to:</p> <ul style="list-style-type: none"> • Understand the need for good security practices. • Identify and assess security risks. • Report security incidents, suspicious behaviour and suspicious packages or baggage. • Conduct facility and vessel security inspections. • Respond to bomb threats. • Implement company security practices. • Carry out procedures for unclaimed/unattended luggage. • Comply with procedures for the acceptance, handling and carriage of luggage on vessels. • Carry out emergency response and evacuation procedures. <p>Reinforce training outcomes at higher threat levels.</p> <p>Check and record staff (permanent, casual and contractor) security awareness training.</p> <p>Reward staff for good security practice – follow up on reports and provide back to staff about what has been done in response.</p> <p>Practise company security and emergency response procedures regularly.</p> <p>Participate in multi agency emergency management exercises.</p>
<p>Ferry and Charter Vessel wharfs and Interchanges</p>	
<p>Wharves and Interchanges are safe and secure.</p> <p>Weapons or explosives do not pose a threat to your operations.</p>	<p>Liase and assist the designated place manager to:</p> <ul style="list-style-type: none"> • Develop consistent and integrated security and emergency response procedures. • Assist in facilitate police/security patrols on a risk based approach. Increase the frequency of inspections at higher levels of alert. • Inspect high-density interchanges at least twice a day to ensure that there are no suspicious items or evidence of illegal activity within your own area –

<p><u>Security Outcomes</u></p>	<p><u>Possible Security Measures</u> BLUE At LOW and MEDIUM Alert, add AMBER at HIGH Alert, and add RED at EXTREME Alert</p>
<p>The right vessels access wharfs/ interchanges and termini</p>	<p>Increase the frequency of inspections at higher levels of alert.</p> <ul style="list-style-type: none"> • Remove bike lockers and other large receptacles from high passenger density public thoroughfares and assembly areas. • Keep facilities clean, well lit and free from damage. • Remove all rubbish bins from high density public thoroughfare and assembly areas under the control of operators. <p>Report all vessels illegally approaching and/or berthing at wharves/interchanges to police.</p>
<p>Ferries and Charter Vessels</p>	
<p>Timely communication of information.</p> <p>Weapons or explosives are not present in your ferries.</p> <p>CCTV aids to deter, detect and to apprehend offenders.</p> <p>See CCTV Guidelines at: www.lawlink.nsw.gov.au/cpd and www.coag.gov.au/meetings/140706/docs/cctv_code_practice.rtf</p>	<p>Establish effective and routine communications with ferries and charter vessels in transit - Increase the frequency of reporting at higher threat levels or for specific destinations.</p> <p>Place tamper evident single use seals on items such as equipment boxes fire extinguisher enclosures and life vest storage areas.</p> <p>Undertake pre-departure searches of vessels for suspicious items. Undertake random searches of vessels in service for suspicious packages – Increase frequency at higher levels of alert – check all in-service ferries before they enter major interchanges.</p> <p>Secure unattended vessels berthed alongside. Conduct a search of the vessel before it re-enters service. On the advice of police, suspend or vary services.</p> <p>Where CCTV is installed ensure that:</p> <ul style="list-style-type: none"> • The systems are fully operational. • Cameras are aimed correctly to cover the intended field of view. There is sufficient image storage space in digital systems – archive then delete unwanted images. • VHS systems and tapes are maintained in accordance with the manufacturer’s recommendations. • Any recorded images indicating suspicious behaviour are retained for police assessment. • Consideration is given to the CCTV Guidelines.

<p><u>Security Outcomes</u></p>	<p><u>Possible Security Measures</u> BLUE At LOW and MEDIUM Alert, add AMBER at HIGH Alert, and add RED at EXTREME Alert</p>
<p>Ferry Terminals</p>	
<p>Your facilities are secure. The right vehicles access the right parts of your depot.</p> <p>Vehicles access the depot at the time and place they are required to.</p> <p>Vehicles leave your depot when their authorised business or activity is completed.</p> <p>Your infrastructure denies easy placement or hiding of bombs, weapons or any other security threat.</p> <p>Access to important areas is limited to authorised people.</p> <p>Staff respond appropriately to fires.</p> <p>CCTV aids to deter, detect and to apprehend offenders.</p>	<p>Establish an effective security perimeter and signage, with access control points – Consider staffed at higher security alert levels.</p> <p>Undertake routine security perimeter checking, report breaches and rapidly repair damage - Patrolling at higher alert levels.</p> <p>Clearly define visitor, staff and contractor parking areas – consider parking areas outside the security perimeter – deny access to all but critical vehicle movements at higher levels of alert.</p> <p>Consider time in and time out booking for visitor and staff vehicles entering and leaving terminal/ facility areas - check access authorisation at higher levels of security alert.</p> <p>Inspect operational areas and your administration areas at least once a day to ensure that there are no suspicious items or evidence of illegal activity.</p> <p>Keep your facilities clear of unnecessary fixtures and stores. This way they can be quickly and easily searched, and it will be easier to determine whether there has been any unauthorised access.</p> <p>Conduct a key muster. Ensure all important keys, including duplicates, are accounted for. The lock of any key that cannot be accounted for should be changed and new keys issued.</p> <p>Exercise strict control over master keys, and do not issue a master key to anyone who:</p> <ul style="list-style-type: none"> • Does not have a real need. • Is not an employee. • Is likely to take the key away, incurring the risk of loss or unauthorised duplication. <p>Where fitted, test Access Control systems to ensure that:</p> <ul style="list-style-type: none"> • Barriers close quickly and effectively. • Fittings are robust and secure.

<p><u>Security Outcomes</u></p>	<p><u>Possible Security Measures</u> BLUE At LOW and MEDIUM Alert, add AMBER at HIGH Alert, and add RED at EXTREME Alert</p>
	<ul style="list-style-type: none"> • Access privileges are up to date and lost passes (including passes unaccounted for) and unauthorised persons are programmed out of the system. <p>Ensure all fire suppression/fighting systems and appliances are on hand and are serviceable. Ensure that employees can operate first response fire equipment.</p> <p>Refer to the suggested CCTV practices under the “Ferries” section.</p>
<p>Vessel and Charter Vessel Baggage</p>	
<p>The baggage is received and stored in the right way.</p> <p>The right baggage is in your ferry or terminal.</p> <p>The right baggage is loaded on the right ferry in the right way.</p>	<p>Remove luggage lockers.</p> <p>Only carry baggage belonging to passenger actually travelling on the vessel. Only accept baggage from persons who have shown photographic identity and have details of identity recorded.</p> <p>Inform passengers that dangerous goods will not be carried using signage and/or pre-printed tickets.</p> <p>Ensure vessel baggage compartments are locked when not being loaded. Supervise the loading and unloading of the luggage compartment (if fitted) to ensure that no unauthorised items are placed in the compartment.</p> <p>Consider tamper proof seals on accessible compartments.</p>

ANNEX B TO SECURITY GUIDELINES

**VESSEL
SECURITY
PLAN**

**For the guidance and information
of operators of NON-SECURITY
REGULATED vessels to assist
in complying with the Safety Management
System (SMS).**

**Non-Security regulated vessels
Include commercial vessels of
less than 500 tons not on an inter-state
voyage.**

IDENTIFICATION OF VESSEL

Name of vessel covered by plan

Registration number of vessel

Vessel Type

Radio Call Sign

Year built

Length of Vessel

Breadth of Vessel

Number of crew (Minimum and Maximum crewing levels)

Number of Passengers

CONTACT DETAILS FOR THE VESSEL OWNER/OPERATOR

Vessel Operator Details

Name of Vessel Operator

Physical address

Mailing address (if different)

Owner details

Name of Owner/Chief Executive Officer

Office Phone Number

Mobile phone Number

Fax Number

e-mail address

Business address

Mailing address (if different)

24 Hour Security contact number.

1. Vessel Operations.

This section should describe the normal operating parameters of the vessel including its business or trade and its operating environment

2. Communication.

This part of the plan should set out the communication procedures relating to the vessel. Particularly in relation to emergencies and security incidents.

3. Vessel Security Records.

Records of any security related incident. Vessel security plans and procedures. Should be kept with the vessel unless not practicable to do so.

4. Reporting Maritime Transport Security Incidents.

Plan should contain procedures for reporting maritime security incidents to the appropriate authorities.

5. Review and Audit.

This section should be used to explain how the operator will ensure the plan is effective and adequate, and that the plan will be implemented correctly. Should include Review and Audit timetable and a record of reviews and audits.

6. Drills and Exercises.

Plan should include procedures for conducting drills and exercise, a proposed timetable for conducting them and a record of the results of the drills and exercises.

7. Duties and Responsibilities.

Sets out the requirements for personnel with a responsibility for security.

8. Knowledge and Training.

*Details the knowledge skills and requirements for the security related aspects of each position. This should detail the training and qualifications that satisfy those requirements and the training that should be given to those personnel
Reference a training register to record which staff have received the appropriate training or have sufficient knowledge to perform their duties.*

9. Security Assessment..

To provide an understanding of security risks and possible preventive security measures and procedures to treat the identified risks.

10. Security Measures and Procedures.

Plan should detail effective measures and procedures to treat security risks and to control access to operating areas of the vessel. It should include procedures for responding to security incidents/threats and for reporting security incidents.

11. Additional Information and Contact Details.

To be completed fully!

Suggest:

NSW Police Marine Area Command (with point of contact)

NSW Maritime (with point of contact)

Commercial Vessel Association

Sydney Ferries Corporation

Standards Australia (for AS/NZS 4360:2004 and the Guidance Handbook)
www.standards.org.au

Need to include link to Dept. of Infrastructure for info on risks assessments, security plans and threat assessments/ transport risk statements. www.infrastructure.gov.au

CCTV Guidelines (State and Federal)

State: www.lawlink.nsw.gov.au/cpd

Federal: www.coag.gov.au/meetings/140706/docs/cctv_code_practice.rtf