



Australian Government

Department of Infrastructure and Transport

**INDUSTRY CODE OF PRACTICE FOR THE REPORTING OF
MARITIME SECURITY EVENTS**

Office of Transport Security

January 2009

CONTENTS

| | |
|---|-----------|
| PART A: INTRODUCTION | 3 |
| 1.0 Purpose of the Code (what is a security event)..... | 3 |
| 2.0 What does the Code cover?..... | 4 |
| 3.0 Who the Code is aimed at..... | 4 |
| 4.0 Definitions | 5 |
| PART B: STANDARDS OF PRACTICE | 5 |
| 5.0 Suggested standards for reporting maritime security events | 5 |
| 6.0 Grades of maritime security events..... | 5 |
| 7.0 Content of reports | 7 |
| 8.0 Reporting timeframes..... | 8 |
| 9.0 Records maintenance | 8 |
| 10.0 Reporting to the Department..... | 9 |
| PART C: COMMENCEMENT & NON-COMPLIANCE..... | 9 |
| PART D: DEPARTMENT'S ROLES AND RESPONSIBILITIES | 9 |
| 12.0 Roles and Responsibilities | 9 |
| ANNEX: LEGISLATIVE FRAMEWORK FOR REPORTING AND MAINTAINING RECORDS | 11 |
| 14.0 Duties and responsibilities of security officers..... | 11 |
| 15.0 Ship security records for regulated Australian ships | 11 |
| 16.0 Procedures for reporting | 12 |

INDUSTRY CODE OF PRACTICE FOR THE REPORTING OF MARITIME SECURITY EVENTS (the Code)

PART A: INTRODUCTION

What is a maritime security event?

A 'maritime security event' is a threatened or actual interference with maritime transport. It is an occurrence (or occurrences), which threatens the security of the maritime industry participant's facility and/or operations AND is not a 'maritime transport or offshore facility security incident'.

How is a maritime security event different from a maritime security incident?

Section 170 of the *Maritime Transport and Offshore Facilities Security Act 2003* (the Act) defines a maritime security incident as a threatened or actual interference with maritime transport which is, or is likely to be, a terrorist act.

Event reporting contributes to the information that the Department of Infrastructure and Transport (the Department) collects and uses to develop a national picture of incident and event occurrences. This enables the Department to identify and analyse trends and policy gaps and provides information that can assist industry to focus security planning around identified risks and vulnerabilities.

1.0 Purpose

- 1.1 The purpose of the Code is to provide guidance to maritime industry participants on how to report 'maritime security events' to the Department.
- 1.2 The Government strongly encourages the reporting of security events which are not 'maritime transport or offshore facility security incidents' as defined under section 170 of the Act¹. Having information on 'maritime security events' will allow the Department to:
 - develop a trend analysis of events across Australia's maritime sector;
 - analyse, assess and advise on the adequacy of a MIP's security plan; and
 - provide analysis reports to maritime industry participants to assist in reviews of their security plans and measures.
- 1.3 The Code is separate to, and does not alter in any way, the reporting requirements for 'maritime transport or offshore facility security incidents'. There are legislative requirements to report maritime transport or offshore facility incidents which are set out in Part 9 of the Act, and the *Maritime Transport and Offshore Facilities Security Act Notice About How Incident Reports Are To Be Made* (No. 3).
- 1.4 Even though it is non-binding, the Department recommends that maritime industry participants comply with the reporting procedures contained in the Code. Maritime industry participants should note that if they voluntarily choose to adopt the Code into their security plans (guidance as to which is set out in the Implementation Strategy) they will need to comply with the procedures as set out in the Code.

¹ A definition of 'maritime transport and offshore facility security incidents' is provided in the Annex section of this Code.

This is because the Act imposes penalties where maritime industry participants fail to comply with their security plans (see for example, section 44).

2.0 What does the Code cover?

2.1 The Code is not legally binding, but sets out standards of practice for:

- reporting 'maritime security events' to the Department; and
- maintaining records of these events.

2.2 How can I identify a reportable maritime security event?

Reportable maritime security events may include, but are not limited to:

- unauthorised or attempted unauthorised access to a maritime, ship or offshore security zone;
- any breach of a screening point that is likely to, or results in persons, vehicles or vessels gaining unauthorised access into a maritime security zone. (This does not include the successful detection of weapons or prohibited items at a screening point);
- inappropriate use of a maritime security identity card to gain, or attempt to gain, access to a maritime, ship or offshore security zone;
- damage to security equipment through sabotage or vandalism;
- unauthorised disclosure of a maritime or ship or offshore security plan;
- unauthorised or attempted unauthorised carriage of weapons or prohibited items in a maritime, ship or offshore security zone;
- suspicious behaviour by persons in or near a regulated entity;
- unexplained or suspicious cargo, goods or luggage in, or in the vicinity of, a maritime, ship or offshore security zone;
- unsecured access points;
- maritime security events during, or after, which the media was present or inquiries by the media were known to have been made; and
- conduct by a person or persons which would, or is likely to, hinder or obstruct the implementation of a maritime industry participant's security plan.

3.0 Who the Code is aimed at

3.1 The Code is aimed at maritime industry participants who have implemented an approved security plan under the Act and Regulations. This includes the following participants with security plans:

- Port operators, port facility operators and port service providers;
- Ship's masters and ship operators; and

- Offshore facility operators and offshore service providers.
- 3.2 Other persons who have incident reporting responsibilities (under section 175 of the Act) and employees of maritime industry participants (under section 176), are encouraged to report maritime security events to the appropriate maritime industry participant's security officer. These reports will help to identify security risks that may need to be addressed.

4.0 Definitions

- 4.1 The terms used in the Code have the same meaning as given in section 10 of the Act and regulation 1.03 of the Regulations.

PART B: STANDARDS OF PRACTICE

Event reporting is an important element of the information base the Department collects and uses to assist industry in its security planning. Analysis of past incidents and security events is a means of identifying trends and provides an effective tool upon which to base future planning considerations.

Achieving effective standards of practice for reporting and maintaining records of maritime security events will assist the Department in receiving a greater amount of higher quality information in a timely manner.

The more complete the information the Department receives, the more detailed analysis can be conducted and therefore the more comprehensive the advice that can be provided to industry.

5.0 Suggested standards for reporting maritime security events

- 5.1 Maritime security events can vary markedly in their seriousness and impact, as evidenced by the list of examples under clause 2.2 of the Code. To account for these differences, suggested reporting standards have been devised for three separate grades of maritime security events (refer to clause 6.0)² to assist in the reporting of them. These standards are set out in Table 1.

6.0 Grades of maritime security events

- 6.1 Grade 1 events are those events that are routine in nature and have been readily resolved (i.e. cause of security threat or breach has been identified and addressed by maritime industry participant). Routine or no follow-up action would normally be involved in such events.
- 6.2 Grade 2 events are those events where the awareness and the assistance of the Department in a guidance and/or compliance capacity is desirable³. Grade 2

² This grading system is provided as a guide only. The maritime security environment is complex and dynamic and the Department encourages the reporting of maritime security events as promptly as possible regardless of their apparent seriousness.

³ The Department is not a response agency. For situations requiring a response, the police and other emergency services should be immediately notified where appropriate.

events include unresolved events where the maritime industry participant is unable to establish or identify:

- the cause of the security threat or breach; and/or
- any action taken to remedy the security threat or breach.

6.3 Grade 3 events are those events where the immediate awareness and possible intervention by the Department is desirable.

6.4 In relation to Grade 2 and 3 events it may also be wise for maritime and/or offshore industry be made aware of them, either generally or for specific maritime industry participants (as the case requires).

Table 1: Standards of practice for reporting maritime security events

| Indicative notification trigger | Suggested timing | Suggested details to be included (if known) |
|---|---|---|
| <p>Maritime Security Event – Grade 1</p> <p>Events which seem to require either routine or no follow-up action.</p> | <p>Monthly reporting – events submitted to the Department (within 14 days after the end of each month).</p> <p>Events that have been reported previously by the maritime industry participant would not normally be repeated in such monthly reporting.</p> | <p>(a) The MIP to whom the report relates.</p> <p>(b) The date and time of the event.</p> <p>(c) The location of the event.</p> <p>(d) If the event involved a ship, information regarding the ship including (if known): name, type, size, flag, IMO number, ISSC number, and type of cargo.</p> |
| <p>Maritime Security Event – Grade 2</p> <p>Events which seem to require awareness and assistance of the Department.</p> | <p>As soon as possible* ideally this means:</p> <ul style="list-style-type: none"> • Notify within 24 hours • Submit oral or written report within 72 hours. | <p>(e) If the event involved a building or other infrastructure, information sufficient to identify the building or other infrastructure, such as the building number, or other identifier.</p> <p>(f) The nature of the event.</p> <p>(g) If the event involved any other MIPs, details of the other MIP(s) involved.</p> <p>(h) A description of the event.</p> <p>(i) If the report is being made on behalf of (including as a result of being notified by) another person or organisation, the name of the person on whose behalf the report is being made.</p> |
| <p>Maritime Security Event – Grade 3</p> <p>Events which seem to require immediate awareness and possible intervention by the Department</p> | <p>As soon as possible.* Ideally, this means:</p> <ul style="list-style-type: none"> • Notify within 4 hours. • Submit written report with required information within 72 hours. | <p>(j) If the person reporting the event is aware that the event has previously been reported to the Department, the approximate time at which the event was reported.</p> <p>(k) An indication of whether the person reporting the event is aware of the event being previously reported to the Police and other MIPs involved as identified in (g).</p> |
| <p>Maritime Transport or Offshore Facility</p> | <p>As soon as possible.* Ideally, this means:</p> <ul style="list-style-type: none"> • Notify within 4 hours. | <p>(l) The name of the person reporting the event.</p> |

| | | |
|--------------------------|--|--|
| Security Incident | <ul style="list-style-type: none"> • Submit written report with required information within 72 hours. | <ul style="list-style-type: none"> (m) The title or position of the person reporting the event. (n) The name of the employer of the person reporting the event, where applicable. (o) The date of the report. |
|--------------------------|--|--|

* Ideally, this means notifying and/or reporting to the Department, when able to do so, yet without compromising the incident/event response.

7.0 Content of reports

7.1 Maritime industry participants' security officers are encouraged to provide the specified information, as set out in column 3 in Table 1, when reporting a maritime security event to the Department's OTS Transport Security Coordination Centre.

7.2 The suggested information, and the reasons why the Department encourages its inclusion, are listed below:

- (a) The maritime industry participant to whom the report relates – the Department needs to know who was involved in the event. Information provided here needs to identify the maritime industry participant in as much detail as possible.
- (b) Date and time of maritime security event - allows the context of analysis to be established and allows timeline-based analysis to be conducted.
- (c) Location of the maritime security event - a fundamental element of reporting and together with the two elements above, forms the basis for analysis. Noting that some maritime industry participants have extensive facilities and even multiple facilities, the event location needs to be identified as specifically as possible.
- (d) Information regarding the ship (where the maritime security event involved a ship) - will be used to categorise events and conduct analysis based on categories such as flag and type. This analysis is very useful in identifying trends and entities who may be involved in repeat events. This information will also assist in identifying foreign flagged ships who may pose a higher risk during future visits to Australia.
- (e) Information sufficient to identify the building or other infrastructure (where the maritime security event involved a building or other infrastructure) – this information will be used in the same manner as data collected for (d) above.
- (f) Identification of the nature of the maritime security event - this is vital for categorisation, trend analysis and indicating the most appropriate direction for future preventive security planning.
- (g) Identification of other maritime industry participant/s involved (if applicable) – this ensures adequate capture of incidents and assists in avoiding a situation where an event may not be correctly reported due to confusion of reporting responsibility. It will also aid in trend and post-event analysis by allowing the Department to identify situations where an event was directed at the industry rather than a single industry participant.

- (h) A description of the maritime security event – this will support the information provided under (f) above. The data will be used in the same way.
- (i) Name of the person or organisation who notified the person reporting the maritime security event (if applicable) – this will allow the tracking of events through the internal reporting mechanisms of the MIP and identify relevant persons for subsequent follow up enquiries.
- (j) Time that the maritime security event was previously reported to the Department (if applicable) – this will ensure that there is not unconnected multiple reporting of events which may result in the corruption of any trend analysis or statistics produced.
- (k) An indication if this event was previously reported to the police and other MIPs involved as identified on (g)
- (l, m) Name and position of the person reporting the maritime security event – this is fundamental in allowing event follow up and authentication of supplied information. The reporting persons contact details should also be provided.
- (n) Name of the employer of the person reporting the maritime security event (if applicable) - to further ensure the integrity of data provided and ensure the capture of the full corporate identity picture of those involved in the event. This will also simplify the follow up process should additional enquiries be required.
- (o) Date of the report – this will allow events to be tracked by reporting dates.

8.0 Reporting timeframes

- 8.1 Maritime industry participants should, if appropriate, immediately contact the police for response action.⁴
- 8.2 The affected maritime industry participant's security officer is encouraged to report the maritime security event to the Department's Transport Security Coordination Centre (TSCC) within the suggested timeframe, as set out in Table 1.

Because information about maritime security events is most useful when it is recent, it is suggested that the Department's TSCC be notified of Grade 2 and 3 events by maritime industry participants as soon as they are able to do so, without compromising the event response. This can be done orally or in writing. It is preferable that a report of the event follow the notification within the timeframe suggested in Table 1.

- 8.3 Where doubt exists as to whether an event should be reported, it is best to report it.

9.0 Records maintenance

- 9.1 The security officer responsible for their maritime industry participant's security plan is encouraged to retain copies of reports, correspondence and any other

⁴ Note: reporting an incident or other maritime security event to the Department is not a substitute for reporting the incident/event to the police and other response agencies.

information relevant to incidents and events affecting the security of the maritime industry participant.

- 9.2 The Department encourages the recording of this information in a format that is able to be easily submitted to the Department's TSCC (refer to clause 10.1 of the Code).

10.0 Reporting to the Department

10.1 Where a maritime security event report is made, it should be sent to the Department's TSCC using one of the following means of communication:

- Telephone – 1300 307 288;
- Telephone from outside Australia - +61 2 6274 8187;
- Facsimile - +61 2 6274 6089;
- E-mail – Transport.security@infrastructure.gov.au; or
- Postal - GPO Box 594, CANBERRA ACT 2601, AUSTRALIA.

PART D: COMMENCEMENT & NON-COMPLIANCE

- 11.1 Maritime industry participants are required, under the Act and Regulations (see Annex to this Code), to address procedures for reporting occurrences which threaten the security of their facility and/or operations.
- 11.2 A way of meeting the requirements for setting out procedures for reporting security occurrences to the Department is by implementation of the Code⁵. However, while strongly encouraged by the Department, it is not compulsory under the Act or Regulations to do so.
- 11.3 However, maritime industry participants who voluntarily choose to adopt the Code into their security plans will need to comply with the procedures as set out in the Code. Please note that the Act imposes penalties where maritime industry participants fail to comply with their security plans (see for example, section 44 of the Act).

PART E: DEPARTMENT'S ROLES AND RESPONSIBILITIES

12.0 Roles and Responsibilities

- 12.1 The Department will undertake to:

⁵ Maritime industry participants should note that the Code only covers reporting security occurrences to the Department and not other relevant authorities. Procedures for reporting to other relevant authorities will need to also be set out in the participant's security plan. The Department recommends that the Code's reporting framework be used as the basis of procedures for reporting to other relevant authorities, but it should be noted that the operation-specific details will vary depending upon the operation in question.

- where appropriate, inform maritime industry participants of information that may affect the implementation of their maritime, ship or offshore security plan;
- where appropriate, provide guidance to assist maritime industry with enhancing their procedures for reporting breaches of security;
- provide analysis and feedback on information submitted by maritime industry participants relating to their reports of maritime security events;
- ensure that a current version of the Code is available and accessible to all affected maritime industry participants from the Department's website; and
- review the Code in cooperation with industry.

ANNEX: LEGISLATIVE FRAMEWORK FOR REPORTING AND MAINTAINING RECORDS

This part of the Code provides an overview of the provisions of the Act and Regulations which are relevant to reporting and maintaining records of security threats and breaches of security. These provisions may also be relevant in the context of maritime security events, especially where the Code is adopted as part of a security plan.

14.0 Duties and responsibilities of security officers

14.1 Security officers appointed by maritime industry participants have specific duties and responsibilities, under the Regulations, in relation to reporting and maintaining records of breaches of security. These include:

- for a port security officer (regulation 1.20(3)(i)) - reporting to the relevant authorities, and maintaining records of, occurrences which threaten the security of the port;
- for a port facility security officer (regulation 1.25(3)(c)(i)) - performing the duties and responsibilities in section 17.2 of Part A of the ISPS Code, which includes reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;
- for a port service provider security officer (regulation 1.30(3)(h)) - reporting to the relevant authorities, and maintaining records of, occurrences which threaten the security of the port service provider;
- for an offshore facility security officer (regulation 1.33(3)(i)) - reporting to the relevant authorities, and maintaining records of, occurrences which threaten the security of the facility;
- for an offshore service provider security officer (regulation 1.34(3)(i)) - reporting to the relevant authorities, and maintaining records of, occurrences which threaten the security of the service provider; and
- for a ship security officer (regulation 1.15(3)(d)(i)) - performing the duties and responsibilities in 12.2 of Part A of the ISPS Code, which includes reporting all security incidents.

15.0 Ship security records for regulated Australian ships

15.1 Under regulation 1.55(1)(j), (k), (l) and (m) of the Regulations, a regulated Australian ship must keep a record of the following information in relation to the ship:

- security threats and maritime transport or offshore facility security incidents;
- breaches of security;
- changes to security levels; and
- communications relating to the direct security of the ship (such as specific threats to the ship or to port or offshore facilities used in connection with the loading or unloading of the ship).

- 15.2 These records must be kept on board the ship for a period of 7 years, as required under regulation 155(4).

16.0 Procedures for reporting

- 16.1 Maritime industry participants' security plans are required, under the Regulations, to address procedures for reporting occurrences which threaten their security as follows:
- a port operator's maritime security plan must address procedures for reporting occurrences which threaten the security of the port - under regulation 3.55(h);
 - a port facility operator's maritime security plan must address procedures for reporting occurrences which threaten the security of the port facility – under regulation 3.125(i);
 - a port service provider's maritime security plan must address procedures for reporting occurrences which threaten the security of the port service provider – under regulation 3.210(i);
 - a ship security plan must address procedures for reporting occurrences which threaten the security of the ship – under regulation 4.45(j);
 - an offshore facility operator offshore security plan must address procedures for reporting occurrences which threaten the security of a facility - under regulation 5A.60(1)(j);
 - an offshore service provider's offshore security plan must address procedures for reporting occurrences which threaten the security of the offshore facility or the offshore service provider (regulation 5A.150(1)(j)).
- 16.3 The Department recommends that a maritime industry participant's security plan include the reporting procedures and requirements contained within this Code, however, merely adopting the Code may not necessarily lead to a plan being accepted. Where a participant does so, they should note that they are required to comply with the procedures set out in the Code, just as they are required to comply with any reporting procedures set out in their security plans. The Act imposes penalties for failing to do so.