Maritime Transport and Offshore Facilities Security Regulations 2003

Statutory Rules 2003 No. 366 as amended

made under the


This compilation was prepared on 29 July 2006
taking into account amendments up to SLI 2006 No. 202

The text of any of those amendments not in force
on that date is appended in the Notes section

Prepared by the Office of Legislative Drafting and Publishing,
Attorney-General’s Department, Canberra
## Contents

### Part 1  Preliminary

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.01</td>
<td>Name of Regulations [see Note 1]</td>
<td>14</td>
</tr>
<tr>
<td>1.02</td>
<td>Commencement [see Note 1]</td>
<td>14</td>
</tr>
<tr>
<td>1.03</td>
<td>Definitions</td>
<td>14</td>
</tr>
<tr>
<td>1.04</td>
<td>Purposes of these Regulations</td>
<td>17</td>
</tr>
<tr>
<td>1.05</td>
<td>Port service providers</td>
<td>18</td>
</tr>
<tr>
<td>1.06</td>
<td>Offshore service providers (Act s 10)</td>
<td>18</td>
</tr>
<tr>
<td>1.10</td>
<td>Company security officers</td>
<td>18</td>
</tr>
<tr>
<td>1.15</td>
<td>Ship security officers</td>
<td>19</td>
</tr>
<tr>
<td>1.20</td>
<td>Port security officers</td>
<td>20</td>
</tr>
<tr>
<td>1.25</td>
<td>Port facility security officers</td>
<td>22</td>
</tr>
<tr>
<td>1.30</td>
<td>Port service provider security officers</td>
<td>23</td>
</tr>
<tr>
<td>1.32</td>
<td>Head security officer</td>
<td>24</td>
</tr>
<tr>
<td>1.33</td>
<td>Offshore facility security officers</td>
<td>25</td>
</tr>
<tr>
<td>1.34</td>
<td>Offshore service provider security officers</td>
<td>26</td>
</tr>
<tr>
<td>1.35</td>
<td>Delegation by security officers</td>
<td>28</td>
</tr>
<tr>
<td>1.40</td>
<td>Shore-based personnel and crew</td>
<td>28</td>
</tr>
<tr>
<td>1.45</td>
<td>Declarations of security</td>
<td>28</td>
</tr>
<tr>
<td>1.50</td>
<td>Security plan audits and reviews</td>
<td>29</td>
</tr>
<tr>
<td>1.55</td>
<td>Ship security records — regulated Australian ships</td>
<td>30</td>
</tr>
<tr>
<td>1.56</td>
<td>Ship security records — regulated foreign ships</td>
<td>32</td>
</tr>
<tr>
<td>1.60</td>
<td>Prohibited items</td>
<td>33</td>
</tr>
<tr>
<td>1.65</td>
<td>Weapon</td>
<td>33</td>
</tr>
<tr>
<td>1.70</td>
<td>Water-side restricted zone</td>
<td>34</td>
</tr>
<tr>
<td>1.75</td>
<td>What are not regulated Australian ships</td>
<td>35</td>
</tr>
<tr>
<td>1.80</td>
<td>What are not regulated foreign ships</td>
<td>35</td>
</tr>
</tbody>
</table>

### Part 2  Maritime security levels and security directions

#### Division 2.1  Preliminary

#### Division 2.2  Maritime security levels

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.25</td>
<td>Notifying maritime security level 2 and 3 declarations and revocations (Act s 32)</td>
<td>36</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>Division 2.3</strong></td>
<td><strong>Security directions</strong></td>
<td></td>
</tr>
<tr>
<td>2.30</td>
<td>Requirement for consultation</td>
<td>36</td>
</tr>
<tr>
<td>2.35</td>
<td>Giving and communicating security directions (Act ss 33 (5))</td>
<td>37</td>
</tr>
<tr>
<td><strong>Part 3</strong></td>
<td><strong>Maritime security plans</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Division 3.1</strong></td>
<td><strong>Preliminary</strong></td>
<td></td>
</tr>
<tr>
<td>3.05</td>
<td>Common requirements for security assessments</td>
<td>38</td>
</tr>
<tr>
<td>3.10</td>
<td>Common requirements for security plan audits and reviews</td>
<td>38</td>
</tr>
<tr>
<td>3.12</td>
<td>Operator to tell Secretary about issuing body for MSICs</td>
<td>39</td>
</tr>
<tr>
<td>3.15</td>
<td>Port operator to give information</td>
<td>39</td>
</tr>
<tr>
<td>3.20</td>
<td>Port facility operator to give information</td>
<td>39</td>
</tr>
<tr>
<td>3.25</td>
<td>Port service provider to give information</td>
<td>40</td>
</tr>
<tr>
<td><strong>Division 3.2</strong></td>
<td><strong>Port operators</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subdivision 3.2.1</strong></td>
<td><strong>Matters to be dealt with in the plan</strong></td>
<td></td>
</tr>
<tr>
<td>3.30</td>
<td>General</td>
<td>41</td>
</tr>
<tr>
<td>3.35</td>
<td>Port operator details</td>
<td>41</td>
</tr>
<tr>
<td>3.40</td>
<td>Security assessments</td>
<td>42</td>
</tr>
<tr>
<td>3.45</td>
<td>Port security officer qualifications and responsibilities</td>
<td>42</td>
</tr>
<tr>
<td>3.50</td>
<td>Other personnel with security role</td>
<td>43</td>
</tr>
<tr>
<td>3.55</td>
<td>Matters that must be in plan</td>
<td>43</td>
</tr>
<tr>
<td>3.60</td>
<td>Consultation and communication</td>
<td>44</td>
</tr>
<tr>
<td>3.65</td>
<td>Maritime security level 1</td>
<td>44</td>
</tr>
<tr>
<td>3.70</td>
<td>Maritime security levels 2 and 3</td>
<td>45</td>
</tr>
<tr>
<td>3.75</td>
<td>Declarations of security</td>
<td>45</td>
</tr>
<tr>
<td>3.77</td>
<td>Land-side restricted zones</td>
<td>45</td>
</tr>
<tr>
<td>3.80</td>
<td>Water-side restricted zones</td>
<td>46</td>
</tr>
<tr>
<td>3.85</td>
<td>Ship security zones</td>
<td>46</td>
</tr>
<tr>
<td><strong>Subdivision 3.2.2</strong></td>
<td><strong>Form of plan</strong></td>
<td></td>
</tr>
<tr>
<td>3.90</td>
<td>Map of port</td>
<td>47</td>
</tr>
<tr>
<td>3.95</td>
<td>Protection of plan</td>
<td>47</td>
</tr>
<tr>
<td><strong>Division 3.3</strong></td>
<td><strong>Port facility operators</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subdivision 3.3.1</strong></td>
<td><strong>Matters to be dealt with in plan</strong></td>
<td></td>
</tr>
<tr>
<td>3.100</td>
<td>Port facility operator details</td>
<td>47</td>
</tr>
<tr>
<td>3.105</td>
<td>Details of other maritime industry participants</td>
<td>48</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>3.106</td>
<td>Obligation to keep information current</td>
<td>48</td>
</tr>
<tr>
<td>3.110</td>
<td>Security assessments</td>
<td>48</td>
</tr>
<tr>
<td>3.115</td>
<td>PFSO qualifications and responsibilities</td>
<td>49</td>
</tr>
<tr>
<td>3.120</td>
<td>Other personnel with security role</td>
<td>49</td>
</tr>
<tr>
<td>3.125</td>
<td>Matters that must be in plan</td>
<td>50</td>
</tr>
<tr>
<td>3.130</td>
<td>Consultation</td>
<td>51</td>
</tr>
<tr>
<td>3.135</td>
<td>Maritime security level 1</td>
<td>51</td>
</tr>
<tr>
<td>3.140</td>
<td>Maritime security levels 2 and 3</td>
<td>52</td>
</tr>
<tr>
<td>3.145</td>
<td>Declarations of security</td>
<td>52</td>
</tr>
<tr>
<td>3.150</td>
<td>Land-side restricted zones</td>
<td>52</td>
</tr>
<tr>
<td>3.155</td>
<td>Cleared zones</td>
<td>53</td>
</tr>
<tr>
<td>3.160</td>
<td>Passenger ships</td>
<td>53</td>
</tr>
<tr>
<td>3.165</td>
<td>Map of port facility</td>
<td>54</td>
</tr>
<tr>
<td>3.170</td>
<td>Protection of plan</td>
<td>54</td>
</tr>
<tr>
<td>Subdivision 3.3.2</td>
<td>Form of plan</td>
<td></td>
</tr>
<tr>
<td>3.165</td>
<td>Map of port facility</td>
<td>54</td>
</tr>
<tr>
<td>3.170</td>
<td>Protection of plan</td>
<td>54</td>
</tr>
<tr>
<td>Division 3.4</td>
<td>Port service providers</td>
<td></td>
</tr>
<tr>
<td>Subdivision 3.4.1</td>
<td>Preliminary</td>
<td></td>
</tr>
<tr>
<td>3.175</td>
<td>Participants required to have maritime security plans</td>
<td>54</td>
</tr>
<tr>
<td>3.180</td>
<td>Certain port service providers not required to have maritime security plans</td>
<td>55</td>
</tr>
<tr>
<td>Subdivision 3.4.2</td>
<td>Matters to be dealt with in plan</td>
<td></td>
</tr>
<tr>
<td>3.185</td>
<td>Port service provider details</td>
<td>55</td>
</tr>
<tr>
<td>3.190</td>
<td>Details of other maritime industry participants</td>
<td>55</td>
</tr>
<tr>
<td>3.191</td>
<td>Obligation to keep information current</td>
<td>56</td>
</tr>
<tr>
<td>3.195</td>
<td>Security assessments</td>
<td>56</td>
</tr>
<tr>
<td>3.200</td>
<td>PSPSO qualifications and responsibilities</td>
<td>57</td>
</tr>
<tr>
<td>3.205</td>
<td>Other personnel with security role</td>
<td>57</td>
</tr>
<tr>
<td>3.210</td>
<td>Matters that must be in plan</td>
<td>57</td>
</tr>
<tr>
<td>3.215</td>
<td>Consultation</td>
<td>58</td>
</tr>
<tr>
<td>3.220</td>
<td>Maritime security level 1</td>
<td>59</td>
</tr>
<tr>
<td>3.225</td>
<td>Maritime security levels 2 and 3</td>
<td>59</td>
</tr>
<tr>
<td>3.230</td>
<td>Declarations of security</td>
<td>59</td>
</tr>
<tr>
<td>3.235</td>
<td>Port security zones</td>
<td>60</td>
</tr>
<tr>
<td>Subdivision 3.4.3</td>
<td>Form of plan</td>
<td></td>
</tr>
<tr>
<td>3.240</td>
<td>Map of port service provider</td>
<td>60</td>
</tr>
<tr>
<td>3.245</td>
<td>Protection of plan</td>
<td>61</td>
</tr>
</tbody>
</table>
Part 4  Ship security plans and ISSCs

Division 4.1  Preliminary

Division 4.2  Matters to be dealt with in ship security plan

4.20  Identification of ship
4.25  Security assessments
4.30  Ship operator, CSO and SSO
4.31  Obligation to keep information current
4.35  Shore-based personnel and crew with security role
4.40  Training
4.45  Matters that must be in plan
4.50  Maritime security level 1
4.55  Maritime security levels 2 and 3
4.60  Declarations of security
4.65  On-board security zones
4.70  Security of ship in non-ISPS Code compliant ports
4.75  Security of ship in exceptional circumstances
4.80  Pre-entry information
4.85  Maritime transport or offshore security incidents
4.90  Security equipment
4.95  On-board systems
4.100  Ship security records
4.105  Security plan audits and reviews

Division 4.3  Form of ship security plan

4.110  Statement about authority of master
4.115  Protection of plan

Division 4.4  Approving, revising and cancelling ship security plans

Division 4.5  International ship security certificates

4.140  Applications for ISSC
4.145  Inspections by authorised persons

Part 5  Regulated foreign ships

Division 5.1  Obligations

5.10  Pre-arrival information
### Division 5.2 Control directions
- **5.20** Requirement for consultation
- **5.25** Giving control directions (Act s 99 (7))

### Part 5A Offshore security plans

#### Division 5A.1 Preliminary
- **5A.05** Common requirements for security assessments
- **5A.10** Common requirements for security plan audits and reviews
- **5A.12** Operator to tell Secretary about issuing body for MSICs
- **5A.15** Offshore facility operator to give information
- **5A.20** Offshore service provider to give information

#### Division 5A.2 Offshore facility operators

##### Subdivision 5A.2.1 Matters to be dealt with in plan
- **5A.25** Offshore security plans (Act s 100H)
- **5A.30** Offshore facility operator details
- **5A.35** Details of offshore service providers
- **5A.40** Obligation to keep information current
- **5A.45** Security assessments
- **5A.50** OFSO qualifications and responsibilities
- **5A.55** Other personnel with security role
- **5A.60** Matters that must be in plan
- **5A.65** Consultation
- **5A.70** Maritime security level 1
- **5A.75** Maritime security levels 2 and 3
- **5A.80** Declarations of security
- **5A.85** Offshore facility zone
- **5A.90** Offshore water-side zone

##### Subdivision 5A.2.2 Form of plan
- **5A.95** Requirements for plans (Act s 100I)
- **5A.100** Information for offshore security plans
- **5A.105** Protection of plan

#### Division 5A.3 Offshore service providers

##### Subdivision 5A.3.1 Preliminary
- **5A.110** Service providers to have offshore security plans (Act s 100B)
Subdivision 5A.3.2 Matters to be dealt with in plan

5A.115 Offshore security plans (Act s 100H) 84
5A.120 Offshore service provider details 85
5A.125 Details of other offshore industry participants 85
5A.130 Obligation to keep information current 86
5A.135 Security assessments 86
5A.140 OSPSO qualifications and responsibilities 86
5A.145 Other personnel with security role 87
5A.150 Matters that must be in plan 87
5A.155 Consultation 88
5A.160 Maritime security level 1 89
5A.165 Maritime security levels 2 and 3 89
5A.170 Declarations of security 89
5A.175 Protection of plan 90

Part 6 Maritime security zones

Division 6.1 Preliminary

6.05 Access not to be denied 91

Division 6.1A Control of maritime security zones

Subdivision 6.1A.1 Preliminary

6.07A Purpose of Division 6.1A 92
6.07B Definitions for Division 6.1A 92
6.07C Meaning of maritime-security-relevant offence 94
6.07D Meaning of valid MSIC 95
6.07E Meaning of properly displaying 96
6.07F Meaning of operational need 96
6.07G Kinds of identification document 96
6.07H Authentication of certain foreign documents 99

Subdivision 6.1A.1A MSIC implementation period

6.07HA Requirements during MSIC implementation period 99
6.07HB MSIC implementation offence 100
6.07HC Powers of maritime security inspectors during MSIC implementation period 101
6.07HD Persons exempted from operation of regulation 6.07HB 102
6.07HE Persons exempted by Secretary from operation of regulation 6.07HB 106
<table>
<thead>
<tr>
<th>Subdivision 6.1A.2 Display of MSICs</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.07I Definitions for Subdivision 6.1A.2</td>
<td>107</td>
</tr>
<tr>
<td>6.07J Requirement to display MSIC in maritime security zones</td>
<td>107</td>
</tr>
<tr>
<td>6.07K Person given disqualifying offence not to enter maritime security zone</td>
<td>108</td>
</tr>
<tr>
<td>6.07L Offence — failure to properly escort visitor</td>
<td>108</td>
</tr>
<tr>
<td>6.07M Persons exempted by Secretary from requirement to hold, carry or display MSIC</td>
<td>109</td>
</tr>
<tr>
<td>6.07N Access by emergency personnel</td>
<td>110</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subdivision 6.1A.3 MSIC issuing bodies</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.07O Application for authorisation to issue MSICs</td>
<td>110</td>
</tr>
<tr>
<td>6.07P Decision on application</td>
<td>111</td>
</tr>
<tr>
<td>6.07Q What an MSIC plan is</td>
<td>111</td>
</tr>
<tr>
<td>6.07R Issuing body to give effect to MSIC plan</td>
<td>112</td>
</tr>
<tr>
<td>6.07S Direction to vary MSIC plan</td>
<td>114</td>
</tr>
<tr>
<td>6.07T Variation of MSIC plan by issuing body</td>
<td>114</td>
</tr>
<tr>
<td>6.07U Inspection of issuing bodies’ MSIC plan and records</td>
<td>115</td>
</tr>
<tr>
<td>6.07V Issuing bodies’ staff</td>
<td>115</td>
</tr>
<tr>
<td>6.07W Revocation of authorisation for cause</td>
<td>116</td>
</tr>
<tr>
<td>6.07X Revocation of authorisation at request of issuing body</td>
<td>117</td>
</tr>
<tr>
<td>6.07Y Re-applying for authorisation</td>
<td>117</td>
</tr>
<tr>
<td>6.07Z What happens if issuing body no longer able to issue MSICs</td>
<td>117</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subdivision 6.1A.4 MSICs: issue, expiry and cancellation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.08A Meaning of adverse criminal record</td>
<td>118</td>
</tr>
<tr>
<td>6.08B MSICs — application for issue</td>
<td>118</td>
</tr>
<tr>
<td>6.08C MSICs — issue</td>
<td>118</td>
</tr>
<tr>
<td>6.08D Issue of disqualifying offence notice</td>
<td>120</td>
</tr>
<tr>
<td>6.08E Issue of MSICs to ASIC holders</td>
<td>121</td>
</tr>
<tr>
<td>6.08F MSICs — Secretary’s approval of issue in certain cases</td>
<td>121</td>
</tr>
<tr>
<td>6.08G Report to Secretary of refusal to issue MSICs in certain cases</td>
<td>122</td>
</tr>
<tr>
<td>6.08H Persons the subject of adverse or qualified security assessments</td>
<td>123</td>
</tr>
<tr>
<td>6.08I MSICs — period of issue and expiry</td>
<td>123</td>
</tr>
<tr>
<td>6.08J Form of MSICs other than temporary MSICs</td>
<td>124</td>
</tr>
<tr>
<td>6.08K Temporary MSICs</td>
<td>126</td>
</tr>
</tbody>
</table>
6.08L  Issue of replacement MSICs  126
6.08M  Cancellation of MSICs  127
6.08N  Cancellation of MSICs at holder’s request  128
6.08O  Report to Secretary of cancellation of MSICs in certain cases  128
6.08P  Return of MSICs that have expired etc  128
6.08Q  Holder no longer needing MSIC  128
6.08R  Notification of lost etc MSICs  129

Subdivision 6.1A.5  Powers of security officers in relation to MSICs

6.08S  Directions to show valid MSICs or other identification  129

Subdivision 6.1A.6  Record-keeping

6.08T  Register of MSICs  130
6.08U  Other records  131
6.08V  Annual reporting  131

Subdivision 6.1A.7  Review of decisions

6.08W  Definitions  132
6.08X  Reconsideration of decisions in relation to MSICs and related matters  132
6.08Y  If Secretary makes no decision  134
6.08Z  AAT review of Secretary’s decisions  134

Subdivision 6.1A.8  Miscellaneous

6.09A  Cost recovery  134

Division 6.2  Port security zones

Subdivision 6.2.1  General

6.20  Types of port security zones  134
6.25  Security barriers  134

Subdivision 6.2.2  Land-side restricted zones

6.30  Identification of zones  135
6.33  Duties of port operator  135
6.35  Duties of port facility operator  136
6.40  Duties of port service provider  136
6.45  Offences — unauthorised entry  136

Subdivision 6.2.3  Cleared zones

6.50  Duties of port facility operator  137
6.55  Identification of zones  137
6.60  Offences — unauthorised entry  137

Subdivision 6.2.4  Water-side restricted zones

6.65  Identification of zones  138
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.70</td>
<td>Duties of port operator</td>
<td>138</td>
</tr>
<tr>
<td>6.75</td>
<td>Offences — unauthorised entry</td>
<td>139</td>
</tr>
<tr>
<td><strong>Division 6.3</strong></td>
<td><strong>Ship security zones</strong></td>
<td></td>
</tr>
<tr>
<td>6.80</td>
<td>Exclusion zones</td>
<td>139</td>
</tr>
<tr>
<td>6.85</td>
<td>Declaration of operation of zone</td>
<td>140</td>
</tr>
<tr>
<td>6.90</td>
<td>Identification of zones</td>
<td>140</td>
</tr>
<tr>
<td>6.95</td>
<td>Duties of port operator</td>
<td>141</td>
</tr>
<tr>
<td>6.100</td>
<td>Offences — unauthorised entry</td>
<td>141</td>
</tr>
<tr>
<td><strong>Division 6.4</strong></td>
<td><strong>On-board security zones</strong></td>
<td></td>
</tr>
<tr>
<td>6.105</td>
<td>On-board restricted areas</td>
<td>142</td>
</tr>
<tr>
<td>6.110</td>
<td>Identification of zones</td>
<td>142</td>
</tr>
<tr>
<td>6.115</td>
<td>Duties of ship operators</td>
<td>142</td>
</tr>
<tr>
<td>6.120</td>
<td>Offences — unauthorised entry</td>
<td>142</td>
</tr>
<tr>
<td><strong>Division 6.5</strong></td>
<td><strong>Offshore security zones</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subdivision 6.5.1</strong></td>
<td><strong>Preliminary</strong></td>
<td></td>
</tr>
<tr>
<td>6.125</td>
<td>Types of offshore security zones (Act s 113B)</td>
<td>143</td>
</tr>
<tr>
<td><strong>Subdivision 6.5.2</strong></td>
<td><strong>Offshore facility zones</strong></td>
<td></td>
</tr>
<tr>
<td>6.130</td>
<td>Identification of zones</td>
<td>143</td>
</tr>
<tr>
<td>6.135</td>
<td>Duties of offshore facility operator</td>
<td>143</td>
</tr>
<tr>
<td>6.140</td>
<td>Offences — unauthorised entry</td>
<td>144</td>
</tr>
<tr>
<td><strong>Subdivision 6.5.3</strong></td>
<td><strong>Offshore water-side zones</strong></td>
<td></td>
</tr>
<tr>
<td>6.145</td>
<td>Identification of zones</td>
<td>144</td>
</tr>
<tr>
<td>6.150</td>
<td>Duties of offshore facility operator</td>
<td>144</td>
</tr>
<tr>
<td>6.155</td>
<td>Offences – unauthorised entry</td>
<td>145</td>
</tr>
<tr>
<td><strong>Part 7</strong></td>
<td><strong>Other security measures</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Division 7.1</strong></td>
<td><strong>Preliminary</strong></td>
<td></td>
</tr>
<tr>
<td>7.05</td>
<td>Access not to be denied</td>
<td>146</td>
</tr>
<tr>
<td><strong>Division 7.2</strong></td>
<td><strong>Screening and clearing</strong></td>
<td></td>
</tr>
<tr>
<td>7.20</td>
<td>Duties of port facility operator</td>
<td>147</td>
</tr>
<tr>
<td>7.25</td>
<td>Persons who need not be screened</td>
<td>147</td>
</tr>
<tr>
<td>7.27</td>
<td>Goods that need not be screened</td>
<td>149</td>
</tr>
<tr>
<td>7.28</td>
<td>Vehicles that need not be screened</td>
<td>149</td>
</tr>
<tr>
<td>7.29</td>
<td>Vessels that need not be screened</td>
<td>149</td>
</tr>
<tr>
<td>7.30</td>
<td>Equipment to be used for screening</td>
<td>150</td>
</tr>
<tr>
<td>7.33</td>
<td>Notice to be displayed at screening points</td>
<td>150</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.35</td>
<td>Offences — screening and clearing</td>
<td>150</td>
</tr>
<tr>
<td>Division 7.3</td>
<td><strong>Weapons and prohibited items</strong></td>
<td></td>
</tr>
<tr>
<td>7.39</td>
<td>Definition of <em>licensed security guard</em> for Division 7.3</td>
<td>152</td>
</tr>
<tr>
<td>7.40</td>
<td>Persons authorised to possess weapons or prohibited items in maritime security zones</td>
<td>152</td>
</tr>
<tr>
<td>7.45</td>
<td>Authorised possession of weapons or prohibited items when passing through screening points</td>
<td>153</td>
</tr>
<tr>
<td>7.50</td>
<td>Authorised carriage or possession of weapons or prohibited items on board regulated Australian ships</td>
<td>155</td>
</tr>
<tr>
<td>7.55</td>
<td>Authorisation subject to compliance with other laws</td>
<td>156</td>
</tr>
<tr>
<td>Part 8</td>
<td><strong>Powers of officials</strong></td>
<td></td>
</tr>
<tr>
<td>Division 8.1</td>
<td>Preliminary</td>
<td></td>
</tr>
<tr>
<td>Division 8.2</td>
<td>Maritime security inspectors</td>
<td></td>
</tr>
<tr>
<td>8.20A</td>
<td>Maritime security inspectors — criteria for appointment</td>
<td>157</td>
</tr>
<tr>
<td>8.20</td>
<td>Identity cards (Act s 137 (2))</td>
<td>158</td>
</tr>
<tr>
<td>Division 8.3</td>
<td>Duly authorised officers</td>
<td></td>
</tr>
<tr>
<td>Division 8.4</td>
<td>Law enforcement officers</td>
<td></td>
</tr>
<tr>
<td>8.40</td>
<td>Customs officers who are law enforcement officers</td>
<td>158</td>
</tr>
<tr>
<td>Division 8.5</td>
<td>Maritime security guards</td>
<td></td>
</tr>
<tr>
<td>8.50</td>
<td>Training and qualifications</td>
<td>159</td>
</tr>
<tr>
<td>8.55</td>
<td>Identity cards (Act s 162 (2) (b))</td>
<td>159</td>
</tr>
<tr>
<td>Division 8.6</td>
<td>Screening officers</td>
<td></td>
</tr>
<tr>
<td>8.60</td>
<td>Training and qualifications</td>
<td>160</td>
</tr>
<tr>
<td>8.65</td>
<td>Identity cards (Act s 165 (2) (b))</td>
<td>161</td>
</tr>
</tbody>
</table>
### Part 9
**Reporting maritime transport or offshore facility security incidents**

### Part 10
**Information-gathering**

### Part 11
**Enforcement**

#### Division 11.2  Infringement notices

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.05</td>
<td>Purpose and effect of Division</td>
<td>163</td>
</tr>
<tr>
<td>11.10</td>
<td>Definition for Division — <em>authorised person</em></td>
<td>163</td>
</tr>
<tr>
<td>11.15</td>
<td>Amount of penalty if infringement notice issued</td>
<td>163</td>
</tr>
<tr>
<td>11.20</td>
<td>Authorised persons may issue infringement notices</td>
<td>164</td>
</tr>
<tr>
<td>11.25</td>
<td>Contents of infringement notice</td>
<td>164</td>
</tr>
<tr>
<td>11.30</td>
<td>Service of infringement notices</td>
<td>165</td>
</tr>
<tr>
<td>11.35</td>
<td>Time for payment of penalty</td>
<td>166</td>
</tr>
<tr>
<td>11.40</td>
<td>Extension of time to pay penalty</td>
<td>166</td>
</tr>
<tr>
<td>11.45</td>
<td>Payment of penalty</td>
<td>167</td>
</tr>
<tr>
<td>11.50</td>
<td>Effect of payment of penalty</td>
<td>167</td>
</tr>
<tr>
<td>11.55</td>
<td>Withdrawal of infringement notice</td>
<td>168</td>
</tr>
<tr>
<td>11.60</td>
<td>Notice of withdrawal of infringement notices</td>
<td>168</td>
</tr>
<tr>
<td>11.65</td>
<td>Refund of penalty etc if infringement notice</td>
<td>169</td>
</tr>
<tr>
<td></td>
<td>withdrawn</td>
<td></td>
</tr>
<tr>
<td>11.70</td>
<td>Evidence of certain matters in relation to</td>
<td>169</td>
</tr>
<tr>
<td></td>
<td>infringement notices</td>
<td></td>
</tr>
<tr>
<td>11.75</td>
<td>Effect of certain admissions</td>
<td>170</td>
</tr>
<tr>
<td>11.80</td>
<td>Matter not to be taken into account in determining</td>
<td>170</td>
</tr>
<tr>
<td></td>
<td>sentence</td>
<td></td>
</tr>
</tbody>
</table>

#### Division 11.6  Demerit points system

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.300</td>
<td>Purpose of Division</td>
<td>171</td>
</tr>
<tr>
<td>11.305</td>
<td>Accrual of demerit points by maritime industry</td>
<td>171</td>
</tr>
<tr>
<td></td>
<td>participants</td>
<td></td>
</tr>
<tr>
<td>11.310</td>
<td>Accumulation of demerit points in respect of ships</td>
<td>171</td>
</tr>
<tr>
<td>11.315</td>
<td>Expiry of demerit points</td>
<td>172</td>
</tr>
<tr>
<td>11.320</td>
<td>Demerit points — maritime security plans</td>
<td>172</td>
</tr>
<tr>
<td>11.325</td>
<td>Demerit points — ship security plans</td>
<td>172</td>
</tr>
<tr>
<td>11.330</td>
<td>Demerit points — offshore security plans</td>
<td>172</td>
</tr>
<tr>
<td>11.335</td>
<td>Register of demerit points</td>
<td>172</td>
</tr>
<tr>
<td>Part 12</td>
<td>Review of decisions</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Part 13</td>
<td>Miscellaneous</td>
<td></td>
</tr>
<tr>
<td>13.05</td>
<td>Ship security alert systems</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td>176</td>
<td></td>
</tr>
</tbody>
</table>

Federal Register of Legislative Instruments F2006C00474
Part 1 Preliminary

1.01 Name of Regulations [see Note 1]
These Regulations are the *Maritime Transport and Offshore Facilities Security Regulations 2003*.

1.02 Commencement [see Note 1]
These Regulations commence as follows:
(a) on 1 January 2004 — Part 1 (except regulations 1.06 and 1.34), 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;

(aa) on 1 March 2006 — regulations 1.06, 1.34, 5A.15, 5A.20 and 5A.35, and Division 5A.3;

(b) on the commencement of Part 2 of the *Maritime Transport Security Act 2003* — the remainder.

1.03 Definitions
(1) In these Regulations:

*airport* has the meaning it has the *Aviation Transport Security Act 2004*.

*Australian Federal Police employee* has the same meaning as AFP employee in subsection 4 (1) of the *Australian Federal Police Act 1979*.

*cleared zone* means a type of port security zone, established by the Secretary under subsection 102 (1) of the Act, that comprises an area of land or water, to which access is controlled, for holding persons and goods, vehicles or vessels that have been screened and cleared.

*contact details*, for a person, includes the person’s business address, mailing address, fixed-line telephone number, mobile telephone number, fax number and e-mail address.
contracting government means a contracting government to the SOLAS Convention.

CSO or company security officer has the meaning given by regulation 1.10.

exclusion zone means a ship security zone, declared by the Secretary to operate under subsection 106 (1) of the Act, that comprises an area of water within a security regulated port, being an area surrounding a security regulated ship (at and below the water level) to which access is controlled.

HSO or head security officer has the meaning given by regulation 1.32.

land-side restricted zone means a type of port security zone, established by the Secretary under subsection 102 (1) of the Act, that comprises an area of land or a structure connected directly or indirectly to land, to which access is controlled, within the boundaries of a port facility or of land under the control of a port operator or port service provider.

maritime security outcome means an outcome set out in subsection 3 (4) of the Act.

member of the Australian Federal Police has the same meaning as in subsection 4 (1) of the Australian Federal Police Act 1979.

offshore facility zone means a type of offshore security zone, established by the Secretary under subsection 113A (1) of the Act, that comprises the space occupied by an offshore facility.

offshore service provider means a person prescribed by regulation 1.06.

offshore water-side zone means a type of offshore security zone established by the Secretary under subsection 113A (1) of the Act, that comprises an area of water surrounding an offshore facility at the distance from the facility specified by the Secretary.

OFSO or offshore facility security officer has the meaning given by regulation 1.33.

on-board restricted area means an on-board security zone, established by the Secretary under subsection 110 (1) of the Act, that comprises an area, to which access is controlled, on board a regulated Australian ship.
Regulation 1.03

**OSPSO** or **offshore service provider security officer** has the meaning given by regulation 1.34.

**PFSO** or **port facility security officer** has the meaning given by regulation 1.25.

**pleasure craft** means a ship that is used, or intended to be used, wholly for recreational or sporting activities.

**port of call** includes an offshore facility.

**port service provider** means a maritime industry participant prescribed under regulation 1.05.

**pre-entry information** has the meaning given by subregulation 4.80 (2).

**PSO** or **port security officer** has the meaning given by regulation 1.20.

**PSPSO** or **port service provider security officer** has the meaning given by regulation 1.30.

**RFSSO** or **regulated foreign ship security officer** means:
(a) the master of a regulated foreign ship; or
(b) an officer on board a regulated foreign ship who is accountable to the master of the ship for:
   (i) ensuring that the ship complies with section 97 of the Act; and
   (ii) liaising with company, ship, port, port service provider and port facility security officers before the ship enters, or while the ship is in, a security regulated port.

**security barrier** has the meaning given by regulation 6.25.

**security plan audit** means an examination of security measures or procedures to determine if a maritime security plan or a ship security plan has been implemented correctly.

**security plan review** means an evaluation of security measures or procedures to determine if a maritime security plan or a ship security plan is effective and adequate.

**ship/facility interface** means the interaction that occurs when a ship interacts with an offshore facility so that the facility is directly and immediately affected by activities involving the movement of persons or goods.
ship/port interface means the interaction that occurs when a security regulated ship is directly and immediately affected by activities involving:
(a) the movement of persons or goods; or
(b) the provision of port services to or from the ship.

shore-based personnel, in relation to a regulated Australian ship, means the body of persons (other than crew) employed by the ship operator for the ship.

SSO or ship security officer has the meaning given by regulation 1.15.

supply base means a place, at a port or airport, where goods or passengers are loaded on to a vessel or aircraft for transport directly from the place to an offshore facility.

water-side restricted zone has the meaning given by regulation 1.70.

working day, in relation to the operations of a maritime industry participant, means a day other than a Saturday, a Sunday, or a day that is a public holiday in the State or Territory where the operations are conducted.

(2) An expression used in these Regulations and in the ISPS Code has in these Regulations the same meaning as in the ISPS Code, unless the contrary intention appears.

1.04 Purposes of these Regulations

The purposes of these Regulations are:
(a) to ensure that maritime, ship and offshore security plans address specific matters that will satisfy the Secretary that the implementation of the plans will make an appropriate contribution towards the achievement of the maritime security outcomes; and
(b) to set out the requirements for maritime, ship and offshore security plans (including matters that must be dealt with in the plans) so that:
  (i) persons preparing maritime, ship and offshore security plans know what they need to do for the plans to receive approval; and
(ii) plans are consistent in terms of layout and general content; and
(iii) the criteria for approval of plans are clear; and

c) to prescribe matters that are required, permitted, necessary or convenient to be prescribed, including:

(i) requirements in relation to the giving of security and control directions; and
(ii) types of port, ship, on-board and offshore security zones; and
(iii) requirements in relation to screening and clearing; and
(iv) kinds of weapons and prohibited items.

1.05 Port service providers

(1) For paragraph (g) of the definition of *maritime industry participant* in section 10 of the Act, an operator of a kind set out in subregulation (2) is prescribed if the operator provides port services to security regulated ships.

(2) For subregulation (1), the following are the kinds of operators:

(a) lighter operator;
(b) barge operator;
(c) line handling boat operator;
(d) pilotage service operator;
(e) tug operator.

1.06 Offshore service providers (Acts 10)

For paragraph (c) of the definition of *offshore industry participant* in section 10 of the Act, a person that manages a supply base is prescribed.

1.10 Company security officers

(1) Before requesting the Secretary to approve a ship security plan, the ship operator for a regulated Australian ship must designate, in writing, a person within the ship operator’s
organisation as security officer (company security officer or CSO) for the ship.

(2) A CSO may be designated by name or by reference to a position.

(3) The duties and responsibilities of a CSO include:
   (a) answering any questions about the ship security plan, and acting as contact officer, during the approval process; and
   (b) implementing and maintaining the ship security plan for the ship; and
   (c) liaising with the SSO for the ship and with port, port service provider and port facility security officers; and
   (d) performing:
      (i) the duties and responsibilities in section 11.2 of Part A of the ISPS Code; and
      (ii) any additional duties and responsibilities set out in the ship security plan.

(4) The ship operator must ensure that a CSO:
   (a) has the knowledge and ability to perform the duties of a CSO; and
   (b) is given the training set out in the ship security plan; and
   (c) is a suitable person to access and handle security information; and
   (d) has the authority to act on instructions received from the Secretary.

Example
A CSO must have the authority to implement security directions or a change in the security level.

1.15 Ship security officers

(1) The ship operator for a regulated Australian ship must designate, in writing, the master, or another crew member, of the ship as security officer (ship security officer or SSO).

(2) An SSO may be designated by name or by reference to a position.
Regulation 1.20

(3) The duties and responsibilities of an SSO include:
(a) maintaining the ship security plan for the ship; and
(b) liaising with the CSO for the ship and with ship, port, port facility and port service provider security officers; and
(c) performing:
   (i) the duties and responsibilities in section 12.2 of Part A of the ISPS Code; and
   (ii) any additional duties and responsibilities set out in the ship security plan.

(4) The ship operator must ensure that an SSO:
(a) has the knowledge and ability to perform the duties of an SSO; and
(b) is given the training set out in the ship security plan; and
(c) is a suitable person to access and handle security information; and
(d) has the authority to act on instructions received from the Secretary or ship operator.

Example
An SSO must have the authority to implement security directions or a change in the security level.

(5) An SSO who is not the master of the ship is accountable to the master of the ship.

1.20 Port security officers

(1) Before requesting the Secretary to approve a maritime security plan, a port operator for a security regulated port must designate, in writing, a person as security officer (port security officer or PSO).

(2) A PSO may be designated by name or by reference to a position.

(3) The duties and responsibilities of a PSO include:
(a) conducting an initial security survey of the port and facilitating the completion of the security assessment for the port operator’s maritime security plan; and
(b) ensuring the development and maintenance of the maritime security plan for the port operator; and
(c) implementing the maritime security plan; and
(d) undertaking regular security inspections of the port to ensure the effectiveness and adequacy of security measures; and
(e) facilitating security plan reviews; and
(f) recommending and incorporating modifications to the maritime security plan in order to:
   (i) correct deficiencies in the plan; or
   (ii) update the plan to take into account changes to the port; and
(g) enhancing security awareness and vigilance of port personnel; and
(h) ensuring that standards for personnel with, or who have been assigned, security duties and responsibilities are met and that adequate training is provided to such personnel; and
(i) reporting to the relevant authorities, and maintaining records of, occurrences which threaten the security of the port; and
(j) liaising with ship, port service provider and port facility security officers; and
(k) coordinating with security, police, fire, ambulance, medical, search and rescue services, as appropriate; and
(l) ensuring that security equipment is properly operated, inspected, tested, calibrated and maintained; and
(m) when requested by an SSO, assisting in confirming the identity of persons intending to board a ship; and
(n) providing advice to the Secretary on the operational and safety aspects of the implementation of security and control directions; and
(o) communicating and coordinating the implementation of security and control directions.

(4) A port operator must ensure that a PSO:
(a) has the knowledge and ability to perform the duties of a PSO; and
(b) is given the training set out in the maritime security plan for the port operator; and
(c) is a suitable person to access and handle security information; and
(d) has the authority to act on instructions received from the Secretary.

1.25 Port facility security officers

(1) Before requesting the Secretary to approve a maritime security plan, a port facility operator must designate, in writing, a person as security officer (*port facility security officer* or *PFSO*) for the port facility.

(2) A PFSO may be designated by name or by reference to a position.

(3) The duties and responsibilities of a PFSO include:
   (a) facilitating the development, implementation, revision and maintenance of the maritime security plan for the port facility operator; and
   (b) liaising with ship, company, port, port service provider and other port facility security officers; and
   (c) performing:
      (i) the duties and responsibilities in section 17.2 of Part A of the ISPS Code; and
      (ii) any additional duties and responsibilities set out in the maritime security plan.

(4) A port facility operator must ensure that a PFSO:
   (a) has the knowledge and ability to perform the duties of a PFSO; and
   (b) is given the training set out in the maritime security plan for the port facility operator; and
   (c) is a suitable person to access and handle security information; and
   (d) has the authority to act on instructions received from the Secretary.
1.30 Port service provider security officers

(1) Before requesting the Secretary to approve a maritime security plan, a port service provider must designate, in writing, a person as security officer (port service provider security officer or PSPSO).

(2) A PSPSO may be designated by name or by reference to a position.

(3) The duties and responsibilities of a PSPSO include:

(a) conducting an initial security survey of the activities of the port service provider and facilitating the completion of the security assessment for the provider’s maritime security plan; and

(b) ensuring the development and maintenance of the maritime security plan for the port service provider; and

(c) implementing the maritime security plan; and

(d) undertaking regular security inspections of the area under the control of the port service provider to ensure the effectiveness and adequacy of security measures; and

(e) recommending and incorporating modifications to the maritime security plan in order to:

   (i) correct deficiencies in the plan; or

   (ii) update the plan to take into account changes to the port service provider; and

(f) enhancing security awareness and vigilance of the port service provider’s personnel; and

(g) ensuring that standards for personnel with, or who have been assigned, security duties and responsibilities are met and that adequate training is provided to such personnel; and

(h) reporting to the relevant authorities, and maintaining records of, occurrences which threaten the security of the port service provider; and

(i) liaising with ship, port, port facility and other port service provider security officers; and

(j) coordinating with security, police, fire, ambulance, medical, search and rescue services, as appropriate; and
part 1 preliminary

Maritime Transport and Offshore Facilities Security Regulations 2003

Regulation 1.32

(k) ensuring that security equipment is properly operated, inspected, tested, calibrated and maintained; and

(l) when requested by an SSO, assisting in confirming the identity of persons intending to board a ship.

(4) A port service provider must ensure that a PSPSO:

(a) has the knowledge and ability to perform the duties of a PSPSO; and

(b) is given the training set out in the maritime security plan for the port service provider; and

(c) is a suitable person to access and handle security information; and

(d) has the authority to act on instructions received from the Secretary.

1.32 Head security officer

(1) Before requesting the Secretary to approve an offshore security plan, an offshore facility operator must designate, in writing, a person within the operator’s organisation as a security officer (a head security officer or HSO) for all the operator’s facilities.

(2) An HSO may be designated by name or by reference to a position.

(3) The duties and responsibilities of an HSO include:

(a) answering any questions about the plan, and acting as contact officer, during the approval process; and

(b) implementing and maintaining the plan for the facility or facilities; and

(c) liaising with the OFSO for each facility and with OSPSOs; and

(d) performing any additional duties and responsibilities set out in the plan.

(4) The offshore facility operator must ensure that an HSO:

(a) has the knowledge and ability to perform the duties of an HSO; and

(b) is given the training set out in the plan; and

Maritime Transport and Offshore Facilities Security Regulations 2003

Federal Register of Legislative Instruments F2006C00474
(c) is a suitable person to access and handle security information; and
(d) has the authority to act on instructions received from the Secretary; and
(e) is located in Australia at a place that is not an offshore facility.

Example for paragraph (4) (d)
An HSO must have the authority to implement security directions or a change in the security level.

1.33 Offshore facility security officers

(1) Before requesting the Secretary to approve an offshore security plan for an offshore facility, an offshore facility operator must designate, in writing, a person as security officer (an OFSO or offshore facility security officer) for the facility.

(2) An OFSO may be designated by name or by reference to a position.

(3) The duties and responsibilities of an OFSO include:
   (a) conducting an initial security survey of the facility and facilitating the completion of the security assessment for the security plan; and
   (b) ensuring the development and maintenance of the security plan; and
   (c) implementing the security plan; and
   (d) undertaking regular security inspections of the facility to ensure the effectiveness and adequacy of security measures; and
   (e) facilitating security plan reviews; and
   (f) recommending and incorporating modifications to the security plan in order to:
      (i) correct deficiencies in the plan; or
      (ii) update the plan to take into account changes to the facility; and
   (g) enhancing security awareness and vigilance of facility personnel; and
(h) ensuring that standards for personnel with, or who have been assigned, security duties and responsibilities are met and that adequate training is provided to the personnel; and

(i) reporting to the relevant authorities, and maintaining records of, occurrences which threaten the security of the facility; and

(j) liaising with ship security officers and offshore industry participants’ security officers; and

(k) coordinating with security, police, fire, ambulance, medical, search and rescue services, as appropriate; and

(l) ensuring that security equipment is properly operated, inspected, tested, calibrated and maintained; and

(m) confirming the identity of persons intending to enter the facility; and

(n) providing advice to the Secretary on the operational and safety aspects of the implementation of security and control directions; and

(o) communicating and coordinating the implementation of security and control directions.

(4) A facility operator must ensure that an OFSO:
   (a) has the knowledge and ability to perform the duties of an OFSO; and
   (b) is given the training set out in the offshore security plan for the facility operator; and
   (c) is a suitable person to access and handle security information; and
   (d) has the authority to act on instructions received from the Secretary.

1.34 Offshore service provider security officers

(1) Before requesting the Secretary to approve an offshore security plan, an offshore service provider must designate, in writing, a person as security officer (an offshore service provider security officer or OSPSO) for the service.

(2) An OSPSO may be designated by name or by reference to a position.
(3) The duties and responsibilities of an OSPSO include:
(a) conducting an initial security survey of the activities of the service provider and facilitating the completion of the security assessment for the security plan; and
(b) ensuring the development and maintenance of the security plan; and
(c) implementing the security plan; and
(d) undertaking regular security inspections of the service provider’s supply base to ensure that the security measures are adequate and as effective as possible; and
(e) facilitating security plan reviews; and
(f) recommending and incorporating modifications to the security plan in order to:
   (i) correct deficiencies in the plan; or
   (ii) update the plan to take into account changes to the facility; and
(g) enhancing security awareness and vigilance of the service provider’s personnel; and
(h) ensuring that standards for personnel with, or who have been assigned, security duties and responsibilities are met and that adequate training is provided to the personnel; and
(i) reporting to the relevant authorities, and maintaining records of, occurrences which threaten the security of the service provider; and
(j) liaising with the security officers of ships and offshore industry participants; and
(k) coordinating with security, police, fire, ambulance, medical, search and rescue services, as appropriate; and
(l) ensuring that security equipment is properly operated, inspected, tested, calibrated and maintained; and
(m) when requested by an OFSO, assisting in confirming the identity of persons intending to enter an offshore facility; and
(n) providing advice to the Secretary on the operational and safety aspects of the implementation of security and control directions; and
Regulation 1.35

(o) communicating and coordinating the implementation of security and control directions.

(4) A service provider must ensure that an OSPSO:
   (a) has the knowledge and ability to perform the duties of an OSPSO; and
   (b) is given the training set out in the security plan for the service provider; and
   (c) is a suitable person to access and handle security information; and
   (d) has the authority to act on instructions received from the Secretary.

1.35 Delegation by security officers

(1) A CSO, SSO, PSO, PFSO, PSPSO, HSO, OFSO or OSPSO may delegate, in writing, some or all of his or her powers (except this power of delegation), functions and duties.

(2) A delegation under this regulation:
   (a) may only be made to a person who has the knowledge and ability to exercise or perform the powers, functions or duties to be delegated; and
   (b) must specify the delegate by name.

1.40 Shore-based personnel and crew

The ship operator for a regulated Australian ship must ensure that shore-based personnel and crew identified in the ship security plan as having security duties and responsibilities:
   (a) have the knowledge and ability to perform their security-related duties and responsibilities; and
   (b) are given the training set out in the plan.

1.45 Declarations of security

(1) A declaration of security involving a ship and another party must be signed and dated by the master of, or SSO for, the ship and:
(a) if the other party to the agreement is also a ship — the master of, or SSO for, that other ship; or
(b) if the other party to the agreement is a port operator — the PSO; or
(c) if the other party to the agreement is a port facility operator — the PFSO; or
(d) if the other party to the agreement is a port service provider — the PSPSO.

(1A) A declaration of security involving an offshore facility and another party must be signed and dated by the operator of, or HSO for, the facility and:
(a) if the other party to the agreement is a ship — the master of, or SSO for, the ship; or
(b) if the other party to the agreement is an offshore industry participant that operates an offshore service — the security officer for the participant.

(2) A declaration of security must set out:
(a) contact details for the parties and signatories to the agreement; and
(b) the period for which the declaration is valid; and
(c) the maritime security level in force for each party.

Note A sample form of a declaration of security will be available on the Department’s web site: www.dotars.gov.au.

(3) A copy of the declaration of security must be kept by a party to the agreement for a period of 7 years beginning on the day after the declaration ceases to be valid.

1.50 Security plan audits and reviews

(1) A security plan audit or review must be conducted in accordance with the schedule, requirements and procedures set out in the maritime, ship or offshore security plan.

(2) A security plan review must be conducted as soon as practicable after a maritime transport or offshore security incident.
(3) The records of each security plan audit or review must be kept for a period of 7 years beginning on the day after the audit or review is concluded.

1.55 Ship security records — regulated Australian ships

(1) A regulated Australian ship must keep a record of the following information in relation to the ship:

(a) the approved ship security plan for the ship;

(b) whether the ship possesses a valid ISSC;

(c) the period of validity, and the name of the issuing authority, of the ISSCs possessed by the ship;

(d) the security level at which the ship is operating;

(e) the security levels at which the ship operated at ports and offshore facilities, and specific periods during which the ship operated at those levels, while conducting ship/port interfaces and ship/facility interfaces;

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

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

(h) if ship security procedures referred to in paragraph (g) were maintained — the procedures and the specific periods during which those procedures were maintained;

(i) training, drills and exercises;

(j) security threats and maritime transport security incidents;

(k) breaches of security;

(l) changes to security levels;

(m) 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);

(n) ship security plan audits and reviews by internal auditors;

(o) periodic review of ship security assessments;

(p) periodic ship security plan reviews;
(q) implementation of any amendments to the ship security plan;
(r) inspection, testing, calibration and maintenance of security equipment (including ship security alert system);
(s) other practical security-related information in accordance with regulation XI-2/9.2.1 of the SOLAS Convention.

(2) For the definition of ship security record in section 10 of the Act, the following are prescribed to be kept on, by and for a regulated Australian ship:
(a) a document made for the purposes of keeping records required under subregulation (1);
(b) any information included in such a document.

(3) Ship security records must be made available for inspection in accordance with the Act and these Regulations.

(3A) Ship security records in relation to the following matters must be made available for inspection at the request of a person who is authorised by a contracting government to inspect the records:
(a) the security level at which the ship is operating;
(b) the security level at which the ship operated in the last 10 ports of call where it conducted ship/port interface or ship/facility interface;
(c) any special or additional security measures that were implemented by the ship in the last 10 ports of call;
(d) any ship security procedures maintained by the ship in the last 10 ports of call where it conducted ship to ship activities;
(e) the name of the person responsible for appointing:
   (i) the ship’s crew; and
   (ii) other persons employed or engaged in any capacity on board the ship and on the business of the ship;
(f) the name of the person who decides how the ship is to be employed;
(g) if the ship is employed under the terms of a charter party or of charter parties, the names of the parties to the charter arrangements;
(h) other practical security-related information (except details of the ship security plan for the ship) in accordance with regulation XI-2/9.2.1 of the SOLAS Convention.

Note The ISSC of a regulated Australian ship may be inspected by:

(a) a person who is authorised by a contracting government (see regulation 4.145); and

(b) a maritime security inspector (see subparagraph 139 (2) (e) (i) of the Act); and

(c) a duly authorised officer (see subparagraph 148 (2) (c) (i) of the Act).

(4) Ship security records must be kept on board the ship for a period of 7 years beginning on:

(a) in the case of a document — the date of the document or, if the document consists of a series of entries, the date when the latest entry is made on the document; or

(b) in the case of information — the date when the information was obtained or, if the information is part of a document that consists of a series of entries, the date when the latest entry is made on the document.

1.56 Ship security records — regulated foreign ships

For the definition of ship security record in section 10 of the Act, the following are prescribed to be kept on, by and for a regulated foreign ship:

(a) confirmation that a valid ISSC, or approved ISSC equivalent under subsection 91 (3) of the Act, is on board the ship;

(b) the name of the authority that issued the ship’s ISSC or approved ISSC equivalent;

(c) the date when the ISSC or approved ISSC equivalent expires;

(d) any document made for the purpose of keeping records in relation to:

(i) the security level at which the ship is operating; and

(ii) the security level at which the ship operated in the last 10 ports of call where the ship conducted ship/port interface or ship/facility interface; and
(iii) whether the ship implemented any special or additional security measures in the last 10 ports of call; and

(iv) whether appropriate security-related procedures were maintained in the last 10 ports of call where the ship conducted ship to ship activities;

(c) the name of the person responsible for appointing:
   (i) the ship’s crew; and
   (ii) other persons employed or engaged in any capacity on board the ship and on the business of the ship;

(f) the name of the person who decides how the ship is to be employed;

(g) if the ship is employed under the terms of a charter party or of charter parties — the names of the parties to the charter arrangements;

(h) other practical security-related information (except details of the ship security plan for the ship) in accordance with regulation XI-2/9.2.1 of the SOLAS Convention.

1.60 Prohibited items

For the definition of prohibited item in section 10 of the Act, the following are prescribed:

(a) an imitation or replica of a firearm;

(b) an imitation or replica of a bomb, grenade, rocket, missile or mine.

1.65 Weapon

(1) For the definition of weapon in section 10 of the Act, a thing set out or described in column 2 of an item in table 1.65 is a weapon.

(2) Despite anything in table 1.65, a flare or other incendiary safety device is not a weapon if it is carried on board a ship or is kept on an offshore facility as part of the ship’s, or facility’s, safety or signalling equipment.
Table 1.65  Weapons

<table>
<thead>
<tr>
<th>Item</th>
<th>Things or description of things</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bombs and grenades</td>
</tr>
<tr>
<td>2</td>
<td>Live rockets or missiles</td>
</tr>
<tr>
<td>3</td>
<td>Things, other than those included in items 1 and 2:</td>
</tr>
<tr>
<td></td>
<td>(a) that are, or in the nature of, explosives or incendiary devices; or</td>
</tr>
<tr>
<td></td>
<td>(b) that contain or expel gas or other irritants (such as tear gas canisters and smoke cartridges), whether or not live</td>
</tr>
<tr>
<td>4</td>
<td>Flame throwers that are of military design, or other devices that are capable of projecting ignited incendiary fuel</td>
</tr>
<tr>
<td>5</td>
<td>Crossbows or other similar devices consisting of a bow fitted transversely on a stock that has a groove or barrel designed to direct an arrow or bolt</td>
</tr>
<tr>
<td>6</td>
<td>Electromagnetic weapons, or other devices made or modified to emit electromagnetic radiation so as to injure or disable a person</td>
</tr>
<tr>
<td>7</td>
<td>Acoustic or light emitting anti personnel devices</td>
</tr>
<tr>
<td>8</td>
<td>Rocket launchers, recoilless rifles, antitank rifles, bazookas or rocket-propelled-grenade-type launchers</td>
</tr>
</tbody>
</table>

1.70  Water-side restricted zone

(1) A port security zone, established by the Secretary under subsection 102 (1) of the Act, that comprises an area of water within a security regulated port is a water-side restricted zone if:

(a) the area is one where a security regulated ship may berth, anchor or moor; and

(b) access to the area is controlled.

(2) A water-side restricted zone extends below the water level to the seabed and under any wharf adjacent to the zone.
1.75 **What are not regulated Australian ships**

For subsection 16 (2) of the Act, a passenger ship (whether or not also a cargo ship) used for overseas or inter-State voyages is not a regulated Australian ship if the ship is a pleasure craft that is not engaged in trade.

1.80 **What are not regulated foreign ships**

For subsection 17 (2) of the Act, a foreign ship that meets the requirements of paragraphs 17 (1) (b) to (d) of the Act is not a regulated foreign ship if:

(a) the ship is owned or operated by a contracting government and is used, for the time being, only on government non-commercial service; or

(b) the ship is a pleasure craft that is not engaged in trade.
Part 2 Maritime security levels and security directions

Division 2.1 Preliminary

Note This Division heading is reserved for future use.

Division 2.2 Maritime security levels

2.25 Notifying maritime security level 2 and 3 declarations and revocations (Act s 32)

(1) This regulation applies to notifying declarations, or revocations of declarations, under Division 3 of Part 2 of the Act.

(2) The Secretary or port operator must notify a declaration or revocation:
   (a) orally (for example, by telephone or radio communication); or
   (b) in writing; or
   (c) by electronic transmission (for example, by facsimile or e-mail).

Division 2.3 Security directions

2.30 Requirement for consultation

If it is reasonable and practicable to do so, the Secretary must consult with the following about giving a security direction that relates to the movement of ships within, or in or out of, a security regulated port or in an offshore water-side zone:

(a) maritime industry or offshore industry participants who will be affected by the direction;

(b) agencies of the Commonwealth, a State or Territory whose operations in the port will be affected by the direction;
(c) persons, other than those mentioned in paragraph (a) or (b), who need to implement, or comply with, the direction.

Examples for paragraph (c)
Harbour masters and PSOs.

2.35 Giving and communicating security directions (Acts 33 (5))

(1) Subject to subsections 35 (2) and 38 (3) of the Act, the Secretary must give a security direction, or notify a person of the revocation of a security direction under subsection 38 (2) of the Act:

(a) orally (for example, by telephone or radio communication); or

(b) in writing; or

(c) by electronic transmission (for example, by facsimile or e-mail).

Note Under subsection 33 (4) of the Act, a security direction has no effect until the Secretary commits the direction to writing.

(2) Each of the following:

(a) a port operator required to communicate a security direction under subsection 35 (3) of the Act;

(b) an offshore facility operator required to communicate a security direction under subsection 35 (8) of the Act;

(c) a ship operator required to communicate a security direction under subsection 36 (2) of the Act;

must do so using any of the means set out in subregulation (1).
Part 3 Maritime security plans

Division 3.1 Preliminary

3.05 Common requirements for security assessments

A security assessment for a maritime security plan must include the following matters:
(a) the date when the assessment was completed or reviewed;
(b) the scope of the assessment, including assets, infrastructure and operations assessed;
(c) a summary of how the assessment was conducted, including details of the risk management process adopted;
(d) the skills and experience of the key persons who completed or participated in the assessment.

3.10 Common requirements for security plan audits and reviews

A maritime security plan for a port operator, port facility operator or port service provider must set out:
(a) a schedule of security plan audits by internal and external auditors; and
(b) the circumstances, in addition to the occurrence of a maritime transport security incident, following which a security plan review must be conducted; and
(c) the procedures for conducting a security plan audit, including a process for selecting auditors who are independent of the matters being audited; and
(d) the procedures for conducting a security plan review, including a process for consultation during the review.
3.12 Operator to tell Secretary about issuing body for MSICs

(1) No later than 30 June 2006, a port operator, port facility operator or port service provider must give the Secretary the following information in writing:

(a) if the operator is not an issuing body, the identity of the person who will issue MSICs for the operator;
(b) whether the operator will issue temporary MSICs and, if not, the identity of the person who will issue temporary MSICs for the operator.

(2) The operator must notify the Secretary within 7 days if any information given for subregulation (1) is no longer correct.

3.15 Port operator to give information

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

(a) the information set out in regulation 3.35 (including contact details for the PSO); and
(b) the measures to be used by the port operator to inform persons of the location of maritime security zones established within the boundaries of the security regulated port; and
(c) the measures to confirm the identity of persons who are authorised to have access to maritime security zones established within the boundaries of the security regulated port.

3.20 Port facility operator to give information

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

(a) the information set out in regulation 3.100 (including contact details for the PFSO); and
(b) the measures to be used by the port facility operator to inform persons of the location of any port security zones established within the boundaries of the port facility; and

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

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

3.25 Port service provider to give information

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

(a) the information set out in regulation 3.185 (including contact details for the PSPSO); and

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

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

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

(e) the measures to confirm the identity of persons who are authorised to have access to the land under the control of the port service provider, to any port security zones established within the boundaries of that land and to vessels operated by the provider.
Maritime security plans  
Part 3
Port operators  
Division 3.2  

Regulation 3.35

Division 3.2  Port operators

Subdivision 3.2.1 Matters to be dealt with in the plan

3.30 General
A maritime security plan for a port operator must cover all matters of ship/port interface:
(a) that are to be conducted within the security regulated port; and
(b) that are not covered by a maritime security plan for any other maritime industry participant that conducts operations within, or in connection with, the security regulated port.

3.35 Port operator details
(1) A maritime security plan for a port operator must be accompanied by a document setting out the following information:
(a) name of the port operator;
(b) contact details for the port operator;
(c) name of the Chief Executive Officer of the port operator;
(d) name of the port for which the port operator has been designated;
(e) name of the port’s harbour master;
(f) contact details for the harbour master;
(g) name or position of the person who is to be the PSO for the port;
(h) a single 24-hour fixed-line or mobile telephone number for the PSO.

Note Paragraph 47 (1) (c) of the Act requires a maritime security plan for a port operator to include contact details for the PSO.

(2) A port operator must, within 2 working days after the port operator becomes aware of a change in any of the information given under this regulation, notify the Secretary, in writing, of the change.
Penalty: 20 penalty units.

(3) An offence against subregulation (2) is an offence of strict liability.

3.40 Security assessments

In addition to the matters required under regulation 3.05, the security assessment that must be included in a maritime security plan for a port operator must include the following matters:

(a) a statement outlining the risk context or threat situation for the port;
(b) identification and evaluation of strategically important assets, infrastructure and operations that need to be protected;
(c) identification of possible risks or threats to assets, infrastructure and operations, and the likelihood and consequences of their occurrence;
(d) identification of existing security measures, procedures and operations;
(e) identification of gaps in port-wide security arrangements, including gaps arising from port infrastructure, human factors, policies and procedures;
(f) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

3.45 Port security officer qualifications and responsibilities

A maritime security plan for a port operator must set out:

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

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

(c) the training that must be given to the PSO.
3.50 Other personnel with security role

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

(2) The security duties and responsibilities of personnel so identified must be set out in the plan, together with:
   (a) the knowledge, skills and other requirements for the security-related aspects of their positions; and
   (b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
   (c) the training that must be given to such personnel.

3.55 Matters that must be in plan

A maritime security plan for a port operator must address, in addition to the matters required under regulation 3.10, the following matters:

(a) measures to prevent unauthorised access to any port security zones established, or ship security zones declared, in the security regulated port;
(b) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations in the port;
(c) procedures for responding to any security directions given by the Secretary;
(d) procedures for evacuation of the port in case of security threats or breaches of security;
(e) procedures for drills and exercises associated with the plan;
(f) procedures for interfacing with ship security activities;
(g) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to the port;
(h) procedures for reporting occurrences which threaten the security of the port;
(i) measures to ensure the security of the information contained in the plan;
(j) procedures in case the ship security alert system of a ship is activated while in the security regulated port.

Note: A maritime security plan for a port operator must be accompanied by a map covering the whole security regulated port and showing the port security zones established within the port (see subsections 49 (2) and (3) of the Act and regulation 3.90).

3.60 Consultation and communication

(1) A maritime security plan for a port operator must set out a mechanism for consultation:
(a) between the port operator and each of the maritime industry participants conducting operations within the security regulated port, for the purpose of coordinating their security-related activities; and
(b) between the port operator and its employees (or their representatives) regarding security measures and procedures to be implemented.

(2) A maritime security plan for a port operator must set out how the port operator will give notice under subsections 27 (2) and 35 (4) of the Act.

3.65 Maritime security level 1

A maritime security plan for a port operator must set out, in relation to maritime security level 1:
(a) the security measures, identified in the security assessment for the operation, for implementation at that level; and
(b) the measures that have been implemented; and
(c) a schedule for implementing the measures that have not been implemented; and
(d) any interim measures that will be implemented until the measures referred to in paragraph (c) are fully implemented.
3.70 **Maritime security levels 2 and 3**

A maritime security plan for a port operator must set out, in relation to maritime security levels 2 and 3, the additional security measures that the operator will implement if the Secretary declares that maritime security level 2 or 3 is in force for the port.

3.75 **Declarations of security**

A maritime security plan for a port operator must provide for:

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

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

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

3.77 **Land-side restricted zones**

(1) If a port operator wishes the Secretary to establish a land-side restricted zone, the maritime security plan for the port operator must set out:

(a) the purpose for the proposed establishment of the zone; and

(b) the boundaries of the zone; and

(c) if applicable, the period when, or the circumstances in which, the zone is in force; and

(d) the security measures and procedures to be taken to control access into the zone by people, vehicles or things; and

(e) steps to be taken to inform people that a land-side restricted zone is in force and that entry into the zone without authority is an offence; and

(f) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (d) and (e).
(2) A maritime security plan for a port operator must set out security measures and procedures to monitor and control access to land-side restricted zones, including measures to detect and deter unauthorised access to those zones.

### 3.80 Water-side restricted zones

(1) If a port operator wishes the Secretary to establish a water-side restricted zone, the maritime security plan for the port operator must set out:

- (a) the purpose for the proposed establishment of the zone; and
- (b) the boundaries of the zone; and
- (c) if applicable, the period when, or the circumstances in which, the zone is in force; and
- (d) the security measures and procedures to be taken to control access into the zone by people, vessels or things; and
- (e) steps to be taken to inform people that a water-side restricted zone is in force and that entry into the zone without authority is an offence; and
- (f) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (d) and (e).

(2) A maritime security plan for a port operator must set out security measures and procedures to monitor and control access to water-side restricted zones, including measures to detect and deter unauthorised access to those zones.

### 3.85 Ship security zones

A maritime security plan for a port operator must set out security measures and procedures to monitor and control access to ship security zones, including measures to detect and deter unauthorised access to those zones.
Subdivision 3.2.2 Form of plan

3.90 Map of port

The map of the whole security regulated port that must accompany a maritime security plan for a port operator under subsections 49 (2) and (3) of the Act must be of a size and scale that:

(a) clearly shows the boundaries of the port and the location of any port security zones established, or that the operator wishes to be established or changed, within the area covered by the plan; and

(b) enables the Secretary to gazette the boundaries of the port.

3.95 Protection of plan

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

Division 3.3 Port facility operators

Subdivision 3.3.1 Matters to be dealt with in plan

3.100 Port facility operator details

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

(a) name of the port facility operator;

(b) contact details for the port facility operator;

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

(d) name and location of the port facility;

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

(f) name or position of the person who is to be the PFSO for the facility;
Part 3 Maritime security plans
Division 3.3 Port facility operators

Regulation 3.105

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

Note Paragraph 47 (1) (c) of the Act requires a maritime security plan for a port facility operator to include contact details for the PFSO.

3.105 Details of other maritime industry participants

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

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

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

3.106 Obligation to keep information current

(1) A port facility operator must, within 2 working days after the port facility operator becomes aware of a change in any of the information given under regulation 3.100 or 3.105, notify the Secretary, in writing, of the change.

Penalty: 20 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

3.110 Security assessments

(1) In addition to the matters required under regulation 3.05, a security assessment for a port facility operator’s operation must include the following matters:

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

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

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

(d) identification of existing security measures, procedures and operations;
(e) identification of weaknesses (including human factors) in the infrastructure, policies and procedures;
(f) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

(2) A security assessment for a port facility operator’s operation must consider:
(a) the types of ships, and the types of cargoes transported by ships, served by the port facility; and
(b) any special risks or threats associated with such ships and cargoes.

3.115 PFSO qualifications and responsibilities
A maritime security plan for a port facility operator must set out:
(a) the knowledge, skills and other requirements for the PFSO; and
(b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
(c) the training that must be given to the PFSO.

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

(2) The security duties and responsibilities of personnel so identified must be set out in the plan, together with:
(a) the knowledge, skills and other requirements for the security-related aspects of their positions; and
(b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
(c) the training that must be given to such personnel.
3.125 Matters that must be in plan

(1) A maritime security plan for a port facility operator must address, in addition to the matters required under regulation 3.10, the following matters:

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

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

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

(d) procedures for responding to any security directions given by the Secretary;

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

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

(g) procedures for interfacing with ship security activities;

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

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

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

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

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

(m) procedures for facilitating:

(i) shore leave or relief of crew; and

(ii) access by visitors (including representatives of seafarers’ welfare and of labour organisations).
(2) In determining appropriate measures for paragraphs (1) (a) and (b), the port facility operator must have regard to the special risks or threats associated with the types of ships, and the types of cargoes transported by ships, regularly served by the port facility.

Note: A maritime security plan for a port facility operator must be accompanied by a map showing any port security zones established within the facility (see paragraph 49 (2) (a) of the Act and regulation 3.165).

3.130 Consultation

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

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

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

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

3.135 Maritime security level 1

A maritime security plan for a port facility operator must set out, in relation to maritime security level 1:

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

(b) the measures that have been implemented; and

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

(d) any interim measures that will be implemented until the measures referred to in paragraph (c) are fully implemented.
3.140 Maritime security levels 2 and 3
A maritime security plan for a port facility operator must set out, in relation to maritime security levels 2 and 3, the additional security measures that the operator will implement if the Secretary declares that maritime security level 2 or 3 is in force for the port.

3.145 Declarations of security
A maritime security plan for a port facility operator must provide for:
(a) the circumstances in which the operator will request a declaration of security with a ship; and
(b) the procedures for negotiating the security measures and responsibilities of the operator and of the ship in those circumstances; and
(c) how security measures identified in a declaration will be implemented to ensure compliance by the operator and the ship with their security plans and with the declaration.

3.150 Land-side restricted zones
(1) If a port facility operator wishes the Secretary to establish a land-side restricted zone, the maritime security plan for the port facility operator must set out:
(a) the purpose for the proposed establishment of the zone; and
(b) the boundaries of the zone; and
(c) if applicable, the period when, or the circumstances in which, the zone is in force; and
(d) the security measures and procedures to be taken to control access into the zone by people, vehicles or things, (including measures relating to the entry, parking, loading and unloading of vehicles, and the movement and storage of cargo, stores and baggage); and
(e) steps to be taken to inform people that a land-side restricted zone is in force and that entry into the zone without authority is an offence; and
(f) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (d) and (e).

(2) A maritime security plan for a port facility operator must set out security measures and procedures to monitor and control access to land-side restricted zones, including measures to detect and deter unauthorised access to those zones.

### 3.155 Cleared zones

A maritime security plan for a port facility operator must set out measures and procedures to ensure that persons and goods are screened and cleared in accordance with these Regulations before they are allowed to enter and remain in any cleared zone established in the port facility.

### 3.160 Passenger ships

(1) If a port facility operator wishes to operate a port facility for use in connection with the loading or unloading of security regulated passenger ships, the maritime security plan for the port facility operator must set out:

a) procedures for screening and clearing persons and their baggage; and

b) procedures for detecting weapons and prohibited items; and

c) procedures for surrender and dealing with weapons and prohibited items that are detected; and

d) the name or position of the person or persons responsible for the procedures referred to in paragraphs (a), (b) and (c).

(2) If in a port facility there is no screening point through which persons who are required to be screened and cleared to board a security regulated ship must pass, the procedures for screening and clearing persons referred to in paragraph (1) (a) must include procedures for making arrangements, between the port facility operator and the master of a ship that is moored at the facility, for persons to be screened and cleared on board the ship immediately after they board.
Subdivision 3.3.2 Form of plan

3.165 Map of port facility
The map that must accompany a maritime security plan for a port facility operator under subsection 49 (2) of the Act must be of a size and scale that clearly shows:
(a) the boundaries of the port facility; and
(b) the location of any port security zones established, or that the operator wishes to be established or changed, within the area covered by the plan.

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

Division 3.4 Port service providers

Subdivision 3.4.1 Preliminary

3.175 Participants required to have maritime security plans
For paragraph 42 (c) of the Act, the following kinds of port service providers are prescribed:
(a) port service providers that operate within a security regulated port;
(b) port service providers that operate outside a security regulated port for the purpose of ship/port interface between a security regulated ship and a security regulated port.

Examples
1 For paragraph (a), a port service provider that operates in a security regulated port (even though its office is located outside the port).
2 For paragraph (b), a pilot boat that takes a pilot to board a ship at a location outside the security regulated port for the purpose of enabling the pilot to bring the ship into the port.
3.180 **Certain port service providers not required to have maritime security plans**

A port service provider of a kind prescribed in paragraph 3.175 (a) or (b) need not have a maritime security plan if:

(a) the activities of the port service provider are covered by a maritime security plan (the *covering plan* within the meaning of subsection 45 (3) of the Act) for another maritime industry participant; and

(b) the port service provider has agreed in writing to those activities being covered by the covering plan.

**Subdivision 3.4.2 Matters to be dealt with in plan**

3.185 **Port service provider details**

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

(a) name of the port service provider;

(b) contact details for the port service provider;

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

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

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

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

*Note* Paragraph 47 (1) (c) of the Act requires a maritime security plan for a port service provider to include contact details for the PSPSO.

3.190 **Details of other maritime industry participants**

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

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

3.191 Obligation to keep information current

(1) A port service provider must, within 2 working days after the port service provider becomes aware of a change in any of the information given under regulation 3.185 or 3.190, notify the Secretary, in writing, of the change.

Penalty: 20 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

3.195 Security assessments

In addition to the matters required under regulation 3.05, a security assessment for the operation of a port service provider must include the following matters:

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

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

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

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

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

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

A maritime security plan for a port service provider must set out:

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

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

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

3.205 Other personnel with security role

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

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

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

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

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

3.210 Matters that must be in plan

A maritime security plan for a port service provider must address, in addition to the matters required under regulation 3.10, the following matters:

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

(b) measures to prevent unauthorised access to land in each security regulated port in which the port service provider operates, to any port security zones established within the boundaries of that land and to vessels or helicopters operated or used by the provider;
(c) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations of the port service provider;
(d) procedures for responding to any security directions given by the Secretary;
(e) procedures for evacuation in case of security threats or breaches of security;
(f) procedures for drills and exercises associated with the plan;
(g) procedures for interfacing with ship security activities;
(h) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to the port service provider;
(i) procedures for reporting occurrences which threaten the security of the port service provider;
(j) measures to ensure the security of the information contained in the plan;
(k) measures to ensure security of passengers, cargo and cargo handling equipment under the control of the port service provider;
(l) procedures in case the ship security alert system of a ship is activated while in the security regulated port.

Note A maritime security plan for a port service provider must be accompanied by a map showing any port security zones established within the boundaries of the area under the control of the port service provider (see paragraph 49 (2) (a) of the Act and regulation 3.240).

3.215 Consultation

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

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

(b) between the provider and each port facility operator and port service provider conducting operations within the security regulated port in which the port service provider is located or operates; and
(c) between the provider and any other stakeholder who may be affected by the implementation of the plan; and
(d) between the provider and its employees (or their representatives), regarding security measures and procedures to be implemented.

3.220 Maritime security level 1
A maritime security plan for a port service provider must set out, in relation to maritime security level 1:
(a) the security measures, identified in the security assessment for the operation, for implementation at that level; and
(b) the measures that have been implemented; and
(c) a schedule for implementing the measures that have not been implemented; and
(d) any interim measures that will be implemented until the measures referred to in paragraph (c) are fully implemented.

3.225 Maritime security levels 2 and 3
A maritime security plan for a port service provider must set out, in relation to maritime security levels 2 and 3:
(a) the security measures, identified in the security assessment for the operation, for implementation at those levels; and
(b) the additional security measures that the provider will implement if the Secretary declares that maritime security level 2 or 3 is in force for the port.

3.230 Declarations of security
A maritime security plan for a port service provider must provide for:
(a) the circumstances in which the provider will request a declaration of security with a ship; and
(b) the procedures for negotiating the security measures and responsibilities of the provider and of the ship in those circumstances; and
(c) how security measures identified in a declaration will be implemented to ensure compliance by the provider and the ship with their security plans and with the declaration.

### 3.235 Port security zones

If a port service provider wishes the Secretary to establish or change a port security zone, the maritime security plan for the port service provider must set out:

(a) the purpose for the proposed establishment of, or change in, the zone; and

(b) the boundaries of the zone; and

(c) if applicable, the period when, or the circumstances in which, the zone is in force; and

(d) the security measures and procedures to be taken to control access into the zone by people, vessels or things; and

(e) steps to be taken to inform people that a port security zone is in force and that entry into the zone without authority is an offence; and

(f) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (d) and (e).

*Note* Maritime security zones may be established only within the boundaries of a security regulated port. The Secretary cannot establish a maritime security zone in an area of land or water under the control of a port service provider if the area is not within the boundaries of the security regulated port.

### Subdivision 3.4.3 Form of plan

#### 3.240 Map of port service provider

The map that must accompany a maritime security plan for a port service provider under subsection 49 (2) of the Act must be of a size and scale that clearly shows:

(a) the boundaries of the area under the control of the port service provider; and
(b) the location of any port security zones established, or that the provider wishes to be established or changed, within the area covered by the plan.

3.245 Protection of plan

A port service provider must ensure that the maritime security plan for the provider is protected against unauthorised access, amendment and disclosure.
Part 4 Ship security plans and ISSCs

Division 4.1 Preliminary

Note 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

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

(a) name of the ship;
(b) the ship’s official number, being the number by which the ship is identified in the Australian Register of Ships referred to in section 56 of the Shipping Registration Act 1981;
(c) if the plan is for a regulated Australian ship that is used for overseas voyage — the ship’s IMO ship identification number;
(d) any other distinctive numbers or letters that identify the ship;
(e) type of ship;
(f) radio call sign;
(g) date and port of registry;
(h) year built;
(i) deadweight tonnage;
(j) gross tonnage;
(k) length and breadth of ship;
(l) summer draft;
(m) number of crew;
(n) number of passenger berths;
(o) whether the ship is engaged in overseas or inter-State voyages.
4.25 Security assessments

A ship security assessment for a regulated Australian ship must include the following matters:

(a) the date when the assessment was completed or reviewed;
(b) the scope of the assessment, including assets, infrastructure and operations assessed;
(c) a summary of how the assessment was conducted, including details of the risk management process adopted;
(d) the skills and experience of the key persons who completed or participated in the assessment;
(e) the results of the examination and evaluation of the existing shipboard protective measures, procedures and operations;
(f) a statement outlining the risk context or threat situation for the ship, including consideration of trading routes;
(g) identification and evaluation of key shipboard operations that need to be protected;
(h) identification of possible risks or threats to the key shipboard operations and the likelihood and consequences of their occurrence;
(i) identification of existing security measures, procedures and operations;
(j) identification of weaknesses (including human factors) in the infrastructure, policies and procedures;
(k) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.

4.30 Ship operator, CSO and SSO

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

(a) the name of the ship operator;
(b) the name of the Chief Executive Officer of the ship operator;
(c) the name or position of the person who is to be the CSO for the ship;
(d) a single 24-hour fixed-line or mobile telephone number for the CSO;
(e) the name or position of the person who is to be the SSO for the ship.

Note Paragraph 66 (1) (c) of the Act requires a ship security plan to include contact details for the SSO

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

(3) A ship security plan must set out how the CSO will communicate with the master of the ship if the Secretary or a maritime industry participant acting on behalf of the Secretary:
(a) gives notice that a maritime security level is in force for the ship; or
(b) gives a security direction to the ship.

4.31 Obligation to keep information current

(1) A ship operator must, within 2 working days after the ship operator becomes aware of a change in any of the information given under regulation 4.20 or 4.30, notify the Secretary, in writing, of the change.

Penalty: 20 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

4.35 Shore-based personnel and crew with security role

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

(2) The security duties and responsibilities of personnel and crew so identified must be set out in the plan, together with:
(a) the knowledge, skills and other requirements for the security-related aspects of their positions; and
(b) the training or qualifications that satisfy the requirements referred to in paragraph (a).

### 4.40 Training

A ship security plan must set out the training that a CSO, SSO, and shore-based personnel and crew referred to in regulation 4.35 must receive.

### 4.45 Matters that must be in plan

A ship security plan must address the following matters:

(a) measures to prevent unauthorised carriage or possession of weapons or prohibited items on board the ship;
(b) identification of on-board security zones;
(c) measures to prevent unauthorised access to the ship and any on-board security zones;
(d) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations of ship/port interface;
(e) procedures for:
   (i) acknowledging, and responding to, directions given by the Secretary or a contracting government; and
   (ii) acknowledging notifications of the security level in force from the Secretary or a contracting government;
(f) procedures for evacuation of the ship in case of security threats or breaches of security;
(g) procedures for drills and exercises associated with the plan;
(h) procedures for interfacing with port, port service, port facility and offshore facility security activities;
(i) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to the ship;
(j) procedures for reporting occurrences which threaten the security of the ship;
(k) measures to ensure the security of the information contained in the plan.
4.50 Maritime security level 1

A ship security plan must set out, in relation to maritime security level 1:
(a) the security measures identified in the ship security assessment for implementation at that level; and
(b) the measures that have been implemented; and
(c) a schedule for implementing the measures that have not been implemented; and
(d) any interim measures that will be implemented until the measures referred to in paragraph (c) are fully implemented.

4.55 Maritime security levels 2 and 3

A ship security plan must set out, in relation to maritime security levels 2 and 3:
(a) the security measures identified in the ship security assessment for implementation at those levels; and
(b) the additional security measures that the ship will implement if the Secretary declares that maritime security level 2 or 3 is in force for the ship.

4.60 Declarations of security

A ship security plan must provide for:
(a) the circumstances in which the ship will request a declaration of security with another ship or person; and
(b) the procedures for negotiating the security measures and responsibilities of the ship and of the other ship or person in those circumstances; and
(c) how security measures identified in a declaration will be implemented to ensure compliance by the parties with their security plans and with the declaration.

4.65 On-board security zones

(1) If the ship operator for a regulated Australian ship wishes the Secretary to establish an on-board security zone for the ship, the ship security plan must set out:
(a) the purpose for the proposed establishment of the zone; and
(b) the boundaries of the zone; and
(c) the security measures and procedures to be taken to control access into the zone by people or things; and
(d) steps to be taken to inform people that the on-board security zone has been established and that entry into the zone without authority is an offence; and
(e) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (c) and (d); and
(f) if applicable, the period when, or the circumstances in which, the zone is in force.

(2) A ship security plan must set out security measures and procedures to monitor and control access to on-board security zones, including measures to detect and deter unauthorised access to those zones.

4.70 Security of ship in non-ISPS Code compliant ports

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

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

4.75 Security of ship in exceptional circumstances

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

(1) A ship security plan for a regulated Australian ship that is used for overseas voyage must set out the procedures for giving pre-entry information in accordance with subregulations (2) and (3).

(2) The master of a regulated Australian ship that is due to arrive, from a place outside Australia, at a port in Australia must give the following information (pre-entry information) to a customs officer:

(a) confirmation that a valid ISSC is on board the ship;
(b) the name of the authority that issued the ship’s ISSC;
(c) the date when the ISSC expires;
(d) the maritime security level at which the ship is operating;
(e) the last 10 ports of call where the ship conducted ship/port interface;
(f) whether the ship operated at a security level different from that in paragraph (d), engaged in ship to ship activity, or implemented any special or additional security measures, in the last 10 ports of call;
(g) if known, the next 4 ports of call of the ship (whether in or outside Australia) after the port in relation to which the information is being given.

(3) Pre-entry information must be given at the time the crew report required under section 64ACB of the Customs Act 1901 is given in relation to the port.

Note Section 6 of the Navigation Act 1912 defines overseas voyage as follows:

overseas voyage, in relation to a ship, means a voyage in the course of which the ship travels between:

(a) a port in Australia and a port outside Australia;
(b) a port in Australia and a place in the waters of the sea above the continental shelf of a country other than Australia;
(c) a port outside Australia and a place in the waters of the sea above the continental shelf of Australia;
(d) a place in the waters of the sea above the continental shelf of Australia and a place in the waters of the sea above the continental shelf of a country other than Australia;
(e) ports outside Australia; or
(f) places beyond the continental shelf of Australia.

4.85 **Maritime transport or offshore security incidents**

A ship security plan must set out procedures for:

(a) reporting maritime transport or offshore security incidents to the Secretary; and

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

4.90 **Security equipment**

A ship security plan must:

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

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

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

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

*Note* A ship operator may be guilty of an offence under section 63 (Offence — failing to comply with ship security plan) of the Act if security equipment that is not correctly calibrated is used on board the ship.

4.95 **On-board systems**

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

(a) external and internal communications systems;

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

(c) tracking and positional systems.

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

(a) describe the operational characteristics of the system; and
Regulation 4.100

(b) describe the ship security alert that will be transmitted from the system; and
(c) describe the performance standards to which the system must conform, being standards not below those adopted by the International Maritime Organisation; and
(d) set out the procedures, instructions and guidance for using, testing, activating, de-activating and resetting the system, and for preventing false alarms.

4.100 Ship security records
A ship security plan must set out:
(a) the ship security records that are required to be kept on, by and for the ship in accordance with regulation 1.55; and
(b) a plan for keeping and preserving ship security records; and
(c) the procedures for making those records available for inspection in accordance with subregulation 1.55 (3A).

4.105 Security plan audits and reviews
A ship security plan must set out:
(a) a schedule of security plan audits by internal and external auditors; and
(b) the circumstances, in addition to the occurrence of a maritime transport security incident, following which a security plan review must be conducted; and
(c) the procedures for conducting a security plan audit, including a process for selecting auditors who are independent of the matters being audited; and
(d) the procedures for conducting a security plan review, including a process for consultation during the review.
Division 4.3  Form of ship security plan

4.110 Statement about authority of master

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

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

4.115 Protection of plan

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

Division 4.4 Approving, revising and cancelling ship security plans

Note  This Division heading is reserved for future use.

Division 4.5 International ship security certificates

4.140 Applications for ISSC

(1) For subsection 81 (2) of the Act, an application for an ISSC must be in writing and must:

(a) identify the ship by means of the following:

(i) the name of the ship;
(ii) the ship’s official number, being the number by which the ship is identified in the Australian Register of Ships referred to in section 56 of the Shipping Registration Act 1981;
(iii) if the ship is used for overseas voyages — the ship’s IMO ship identification number;
(iv) any other distinctive numbers or letters that identify the ship; and

(b) include a statement that a ship security plan is in force for the ship.

(2) The application must also state when the ship may be inspected for the purpose of determining whether the ship meets the requirements necessary for ISSC verification.

4.145 Inspections by authorised persons

The ISSC for a regulated Australian ship must be made available for inspection at the request of a person who is authorised by a contracting government to request information about, or in connection with, whether a valid ISSC is in force for the ship.

Note For the power of maritime security inspectors and duly authorised officers to inspect ISSCs, see subparagraphs 139 (2) (e) (i) and 148 (2) (c) (i) of the Act, respectively.
Part 5 Regulated foreign ships

Division 5.1 Obligations

5.10 Pre-arrival information

(1) For subsection 92 (2) of the Act, pre-arrival information must be given to a customs officer by the master of a ship that is due to arrive, from a place outside Australia, at a port in Australia (whether the first port or any subsequent port on the same voyage) at the time the crew report required under section 64ACB of the Customs Act 1901 is given in relation to the port.

(2) For the definition of pre-arrival information in subsection 92 (3) of the Act, the following are prescribed:

(a) confirmation that a valid ISSC, or approved ISSC equivalent under subsection 91 (3) of the Act, is on board the ship;

(b) the name of the authority that issued the ship’s ISSC or approved ISSC equivalent;

(c) the date when the ISSC or approved ISSC equivalent expires;

(d) the security level at which the ship is operating;

(e) the last 10 ports of call where the ship conducted ship/port interface;

(f) whether the ship operated at a security level different from that in paragraph (d), engaged in ship to ship activity, or implemented any special or additional security measures, in the last 10 ports of call;

(g) if known, the next 4 ports of call of the ship (whether in or outside Australia) after the port in relation to which the information is being given.
Division 5.2  Control directions

5.20  Requirement for consultation

If it is reasonable and practicable to do so, the Secretary must consult with the following about giving a control direction that relates to the movement of ships within, or in or out of, a security regulated port:

(a) maritime industry participants who will be affected by the direction;
(b) agencies of the Commonwealth, a State or Territory whose operations in the port will be affected by the direction;
(c) persons, other than those mentioned in paragraph (a) or (b), who need to implement, or comply with, the direction.

Examples for paragraph (c)
Harbour masters and PSOs.

5.25  Giving control directions (Act s 99 (7))

The Secretary must give a control direction to the ship operator for, or the master of, a regulated foreign ship:

(a) orally (for example, by telephone or radio communication); or
(b) in writing; or
(c) by electronic transmission (for example, by facsimile or e-mail).

Note Under subsection 99 (5) of the Act, a control direction has no effect until the Secretary commits the direction to writing.
Part 5A  Offshore security plans

Division 5A.1  Preliminary

5A.05  Common requirements for security assessments
A security assessment for an offshore security plan must include the following matters:
(a) the date when the assessment was completed or reviewed;
(b) the scope of the assessment, including assets, infrastructure and operations assessed;
(c) a summary of how the assessment was conducted, including details of the risk management process adopted;
(d) the skills and experience of the key persons who completed or participated in the assessment.

5A.10  Common requirements for security plan audits and reviews
An offshore security plan for an offshore industry participant must set out:
(a) a schedule of security plan audits by internal and external auditors; and
(b) the circumstances, in addition to the occurrence of a maritime transport or offshore security incident, following which a security plan review must be conducted; and
(c) the procedures for conducting a security plan audit, including a process for selecting auditors who are independent of the matters being audited; and
(d) the procedures for conducting a security plan review, including a process for consultation during the review.

5A.12  Operator to tell Secretary about issuing body for MSICs
(1) No later than 30 June 2006, an offshore facility operator must give the Secretary the following information in writing:
(a) if the operator is not an issuing body, the identity of the person who will issue MSICs for the operator;
(b) if the operator will not issue temporary MSICs, the identity of the person who will issue temporary MSICs for the operator.

(2) The operator must notify the Secretary within 7 days if any information given for subregulation (1) is no longer correct.

5A.15 Offshore facility operator to give information

The operator of an offshore facility must give to each offshore service provider conducting operations at the facility:

(a) the information set out in regulation 5A.30; and
(b) the measures to be used by the operator to inform persons of the location of offshore security zones established by the operator for the facility; and
(c) the measures to confirm the identity of persons who are authorised to have access to the zones.

Note The information for paragraph (a) must include the contact details for the OFSO.

5A.20 Offshore service provider to give information

An offshore service provider that is required to have a security plan must give to the operator of each offshore facility to which the service provider conducts operations:

(a) the information set out in regulation 5A.120; and
(b) a description of the boundaries of the service provider’s supply base and the arrangements made to ensure the security of goods that are to be transported to the facility; and
(c) details of each vessel or aircraft operated by the service provider to service the facility; and
(d) the measures to be used by the service provider to inform persons of the security arrangements, including any security zones, at the service provider’s supply base; and
(e) details of the measures to be used to confirm the identity of persons who are allowed to enter:
(i) the supply base; and
(ii) any security zone established in the supply base; and
(iii) a vessel or aircraft operated by the service provider.

Note The information for paragraph (a) must include the contact details for the OSPSO.

Division 5A.2 Offshore facility operators

Subdivision 5A.2.1 Matters to be dealt with in plan

5A.25 Offshore security plans (Act s 100H)

For section 100H of the Act, this Subdivision prescribes the matters that are to be dealt with in an offshore security plan for an offshore facility operator.

Note An offshore facility operator that has more than 1 facility may prepare 1 plan for each facility, or 1 plan covering a number of facilities that are in the same area, and are physically and operationally similar, and that have identical risk assessments.

5A.30 Offshore facility operator details

An offshore security plan for an offshore facility operator must be accompanied by a document setting out the following information:
(a) the name of the operator;
(b) contact details for the operator;
(c) name of the Chief Executive Officer and the HSO of the operator;
(d) the name and location of each facility;
(e) name or position of the person who is to be the OFSO for each facility covered by the plan;
(f) a single 24-hour fixed-line telephone number, a mobile telephone number and a fax number for the OFSO of the participant.

Note Paragraph 100G (1) (c) of the Act requires an offshore security plan for an offshore industry participant to include details of the participant’s security officer.
5A.35 Details of offshore service providers
An offshore security plan for an offshore facility operator must be accompanied by a document setting out the name of, and contact details for, the OSPSO of each offshore service provider conducting operations at each facility.

5A.40 Obligation to keep information current
(1) An offshore facility operator must, within 2 working days after becoming aware of a change in any of the information given under regulation 5A.30 or 5A.35, notify the Secretary, in writing, of the change.
Penalty: 20 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

5A.45 Security assessments
(1) In addition to the matters required under regulation 5A.05, a security assessment for an offshore facility operator’s operation must include the following matters:
(a) a statement outlining the risk context or threat situation for each facility;
(b) identification and evaluation of important assets, infrastructure and operations that need to be protected;
(c) identification of possible risks or threats to assets, infrastructure and operations, and the likelihood and consequences of their occurrence;
(d) identification of existing security measures, procedures and operations;
(e) identification of weaknesses (including human factors) in the infrastructure, policies and procedures;
(f) identification, selection and prioritisation of possible risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels and vulnerabilities.
(2) A security assessment for an offshore facility operator’s operation must consider:
(a) the types of vessels or aircraft used, and the types of cargoes transported, in operations to and from each offshore facility; and
(b) any special risks or threats associated with the vessels, aircraft and cargoes.

5A.50 OFSO qualifications and responsibilities
An offshore security plan for an offshore facility operator must set out:
(a) the knowledge, skills and other requirements for the OFSO; and
(b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
(c) the training that must be given to the OFSO.

5A.55 Other personnel with security role
(1) An offshore security plan for an offshore facility operator must identify, by reference to their positions, personnel who have been assigned security duties and responsibilities in addition to those of the OFSO.

(2) The security duties and responsibilities of personnel so identified must be set out in the plan, together with:
(a) the knowledge, skills and other requirements for the security-related aspects of their positions; and
(b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
(c) the training that must be given to such personnel.

5A.60 Matters that must be in plan
(1) An offshore security plan for an offshore facility operator must address, in addition to the matters required under regulation 5A.05, the following matters:
(a) measures to prevent unauthorised carriage or possession of
     weapons or prohibited items on a facility or on board
     vessels or aircraft interfacing with a facility;
(b) measures to prevent unauthorised access to an offshore
     security zone;
(c) procedures for responding to security threats or breaches
     of security, including procedures for maintaining critical
     operations at a facility;
(d) procedures for responding to security threats or breaches
     of security occurring during any interface between a vessel
     or aircraft and a facility;
(e) procedures for responding to any security directions given
     by the Secretary;
(f) procedures for evacuation of each facility in case of
     security threats or breaches of security;
(g) procedures for drills and exercises associated with the
     plan;
(h) procedures for interfacing with the security activities of
     other maritime industry participants and operators of any
     aircraft that may land on or near a facility;
(i) procedures for modifying the plan to correct deficiencies
     or to update the plan to take into account changes to a
     facility;
(j) procedures for reporting occurrences which threaten the
     security of a facility;
(k) measures to ensure the security of the information
     contained in the plan;
(l) measures to ensure the security of cargo and of cargo
     handling equipment at a facility;
(m) procedures in case the security alert system of a ship is
     activated while it is near a facility;
(n) procedures to be followed when an offshore facility is
     directly connected to, or engaging in any activity with, a
     vessel such as a floating hotel, mobile drilling unit or
     construction barge.

(2) In determining appropriate measures for paragraphs (1) (a)
     and (b), the facility operator must have regard to the special
     risks or threats associated with the types of vessels and aircraft

used to provide services for each offshore facility and the types of cargo carried by the vessels and aircraft.

5A.65 Consultation

An offshore security plan for an offshore facility operator must set out, for the purpose of coordinating security-related activities, a mechanism for consultation between the offshore facility operator and:

(a) each offshore industry participant conducting operations at (or interfacing with) a facility and any other stakeholder who may be affected by the implementation of the plan; and

(b) the operator’s employees (or their representatives) regarding security measures and procedures to be implemented.

5A.70 Maritime security level 1

An offshore security plan for an offshore facility operator must set out, in relation to maritime security level 1:

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

(b) the measures that have been implemented; and

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

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

5A.75 Maritime security levels 2 and 3

An offshore security plan for an offshore facility operator must set out, in relation to maritime security levels 2 and 3, the additional security measures that the operator will implement if the Secretary declares that maritime security level 2 or 3 is in force for a facility of the operator.
5A.80 Declarations of security

An offshore security plan for an offshore facility operator must provide for:

(a) the circumstances in which the operator will request a declaration of security with another offshore industry participant; and

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

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

5A.85 Offshore facility zone

(1) If an offshore facility operator wishes the Secretary to establish an offshore facility zone for a facility, the offshore security plan for the operator must set out:

(a) the boundaries of the zone; and

(b) the security measures and procedures to be taken to control access into the zone by people, aircraft or things; and

(c) steps to be taken to inform people that an offshore facility zone is in force and that entry into the zone without authority is an offence; and

(d) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (b) and (c).

(2) The security plan must set out security measures and procedures to monitor and control access to the zone, including measures to detect and deter unauthorised access to the zone.

5A.90 Offshore water-side zone

(1) If an offshore facility operator wishes the Secretary to establish an offshore water-side zone for a facility, the offshore security plan for the operator must set out:
(a) the boundaries of the zone; and
(b) the security measures and procedures to be taken to control access into the zone by people, vessels, aircraft or things; and
(c) steps to be taken to inform people that an offshore water-side zone is in force and that entry into the zone without authority is an offence; and
(d) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (b) and (c).

(2) The security plan must set out security measures and procedures to monitor and control access to the zone, including measures to detect and deter unauthorised access to the zone.

Subdivision 5A.2.2  Form of plan

5A.95  Requirements for plans (Act s 100I)
For section 100I of the Act, this Subdivision sets out requirements for the preparation of an offshore security plan.

5A.100  Information for offshore security plans
The information that must accompany an offshore security plan for an offshore facility operator must:
(a) show the location (including the geographical coordinates) of each facility in a way that enables the Secretary to gazette the location of the facility; and
(b) include a diagram of a size and scale of each facility and surrounding water that shows the layout of the facility and of any offshore security zone.

5A.105  Protection of plan
An offshore facility operator must ensure that the offshore security plan for the operator’s facility is protected against unauthorised access, amendment and disclosure.
Division 5A.3 Offshore service providers

Subdivision 5A.3.1 Preliminary

5A.110 Service providers to have offshore security plans (Act s 100B)

(1) For paragraph 100B (b) of the Act, an offshore industry participant that is an offshore service provider is prescribed.

(2) However subregulation (1) does not apply to a service provider if:

(a) the activities of the service provider are covered by the offshore security plan for an offshore facility operator (the covering plan) and the service provider has agreed in writing to the activities being covered by the covering plan; or

(b) both of the following apply:

(i) the activities of the service provider are covered by a maritime security plan, or a transport security program within the meaning given in the Aviation Transport Security Act 2004;

(ii) the service provider has reviewed the plan and, if necessary, amended it to ensure that the provider satisfies the relevant requirements for offshore service providers under these Regulations.

Note Section 100E of the Act deals with the activities of offshore industry participants being covered by offshore security plans of other offshore industry participants.

Subdivision 5A.3.2 Matters to be dealt with in plan

5A.115 Offshore security plans (Act s 100H)

For section 100H of the Act, this Subdivision prescribes the matters that are to be dealt with in an offshore security plan for an offshore service provider.
5A.120 Offshore service provider details

An offshore security plan for an offshore service provider must be accompanied by a document setting out the following information:

(a) the name of the service provider;
(b) contact details for the service provider;
(c) name of the Chief Executive Officer of the service provider;
(d) name of each port or airport:
   (i) where the service provider has a supply base; or
   (ii) from which the service provider operates;
(e) name or position of the person who is to be the OSPSO for the service provider;
(f) a single 24-hour fixed-line telephone number, a mobile telephone number and a fax number for the OSPSO of the participant.

*Note* Paragraph 100G (1) (c) of the Act requires an offshore security plan for an offshore industry participant to include contact details for the OSPSO.

5A.125 Details of other offshore industry participants

An offshore security plan for an offshore service provider must be accompanied by a document setting out the name of, and contact details for:

(a) each PSO of a security regulated port and airport security contact officer (within the meaning given in the *Aviation Transport Security Act 2004*) of a security controlled airport (within the meaning given in that Act):
   (i) where the service provider has a supply base; or
   (ii) from which the service provider operates; and
(b) each OFSO of a security regulated offshore facility serviced by the service provider.
5A.130 **Obligation to keep information current**

(1) An offshore service provider must, within 2 working days after becoming aware of a change in any of the information given under regulation 5A.120 or 5A.125, notify the Secretary, in writing, of the change.

Penalty: 20 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

5A.135 **Security assessments**

In addition to the matters required under regulation 5A.05, a security assessment for an offshore service provider must include the following matters:

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

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

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

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

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

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

5A.140 **OSPSO qualifications and responsibilities**

An offshore security plan for an offshore service provider must set out:

(a) the knowledge, skills and other requirements for the OSPSO; and
(b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
(c) the training that must be given to the OSPSO.

5A.145 Other personnel with security role

(1) An offshore security plan for an offshore service provider must identify, by reference to their positions, personnel who have been assigned security duties and responsibilities in addition to those of the OSPSO.

(2) The security duties and responsibilities of personnel so identified must be set out in the plan, together with:
   (a) the knowledge, skills and other requirements for the security-related aspects of their positions; and
   (b) the training or qualifications that satisfy the requirements referred to in paragraph (a); and
   (c) the training that must be given to such personnel.

5A.150 Matters that must be in plan

(1) An offshore security plan for an offshore service provider must address, in addition to the matters required under regulation 5A.05, the following matters:
   (a) measures to prevent unauthorised carriage or possession of weapons or prohibited items at a supply base of the service provider or on board vessels or aircraft operated by the service provider;
   (b) measures to prevent unauthorised access to a supply base of, or a vessel or aircraft operated by, the service provider;
   (c) procedures for responding to security threats or breaches of security, including procedures for maintaining critical operations of the offshore service provider;
   (d) procedures for responding to security threats or breaches of security occurring during any interface between a vessel or aircraft and a facility;
   (e) procedures for responding to any security directions given by the Secretary;
   (f) procedures for evacuation of a supply base of the service provider in case of security threats or breaches of security;
(g) procedures for drills and exercises associated with the plan;
(h) procedures for interfacing with the security activities of vessels and offshore facilities serviced by the service provider;
(i) procedures for modifying the plan to correct deficiencies or to update the plan to take into account changes to a relevant facility and to the service provider;
(j) procedures for reporting occurrences which threaten the security of the offshore facility or the offshore service provider;
(k) measures to ensure the security of the information contained in the plan;
(l) measures to ensure security of passengers, cargo and cargo handling equipment under the control of the offshore service provider;
(m) procedures in case the ship security alert system of a ship is activated while interfacing with the service provider.

(2) In determining appropriate measures for paragraph (1) (a) and (b), the service provider must have regard to the special risks or threats associated with the types of vessels and aircraft and the types of cargoes transported by vessels and aircraft serving an offshore facility.

5A.155 Consultation

An offshore security plan for an offshore service provider must set out, for the purpose of coordinating security-related activities, a mechanism for consultation between the service provider and:
(a) each offshore facility operator serviced by the service provider; and
(b) the operator of each security regulated port and each airport from which the service provider operates; and
(c) any other stakeholder who may be affected by the implementation of the plan; and
(d) the service provider’s employees (or their representatives), regarding security measures and procedures to be implemented.

5A.160 Maritime security level 1
An offshore security plan for an offshore service provider must set out, in relation to maritime security level 1:
(a) the security measures, identified in the security assessment for the operation, for implementation at that level; and
(b) the measures that have been implemented; and
(c) a schedule for implementing the measures that have not been implemented; and
(d) any interim measures that will be implemented until the measures referred to in paragraph (c) are fully implemented.

5A.165 Maritime security levels 2 and 3
An offshore security plan for an offshore service provider must set out, in relation to maritime security levels 2 and 3, the additional security measures that the service provider will implement if the Secretary declares that maritime security level 2 or 3 is in force for a port or airport at which the service provider operates.

5A.170 Declarations of security
An offshore security plan for an offshore service provider must provide for:
(a) the circumstances in which the service provider will request a declaration of security with another offshore industry participant or a ship; and
(b) the procedures for negotiating the security measures and responsibilities of the service provider and the participant in those circumstances; and
(c) how security measures identified in a declaration will be implemented to ensure compliance by the service provider and the participant with their security plans and with the declaration.
5A.175 Protection of plan

An offshore service provider must ensure that the offshore security plan for the service provider is protected against unauthorised access, amendment and disclosure.
Part 6 Maritime security zones

Division 6.1 Preliminary

6.05 Access not to be denied

(1) Nothing in this Part has the effect of preventing entry into a maritime security zone by a person who:

(a) is accompanied by a law enforcement officer for the purposes of an investigation; or

(b) is an Australian Federal Police employee, a member of the Australian Federal Police, or an officer or employee of the police force or service of a State or Territory, who requires access for the purposes of a police investigation; or

(c) is otherwise authorised by a law of the Commonwealth, State or Territory to enter the maritime security zone.

Example for paragraph (c)
Entry to maritime security zones must not be denied to law enforcement officers, Australian Customs Service officers or AMSA officers if the entry is required in the course of their duties.

(2) Nothing in this Part has the effect of preventing a member of the Australian Defence Force who is on duty:

(a) from entering a maritime security zone; or

(b) from taking into a maritime security zone vessels, vehicles or goods:

(i) for the purpose of gaining access to a ship that is under the control, or in the service, of the Australian Defence Force; or

(ii) in connection with the movement, loading, unloading, maintenance or provisioning of such a ship.
Division 6.1A  Control of maritime security zones

Subdivision 6.1A.1  Preliminary

6.07A  Purpose of Division 6.1A

(1) This Division provides for a scheme under which:
   (a) an MSIC is issued to identify a person who has been the subject of a background check; and
   (b) in the MSIC implementation period a person, other than an exempt person, who enters a maritime security zone must be an MSIC applicant; and
   (c) on or after 1 January 2007, a maritime industry participant will not allow a person to enter, or remain in, a maritime security zone unless the person:
       (i) displays a valid MSIC; or
       (ii) is escorted by the holder of an MSIC.

(2) The Division includes requirements about:
   (a) the display of MSICs; and
   (b) issuing bodies for MSICs; and
   (c) the issue of an MSIC to a person; and
   (d) the expiry and cancellation of MSICs.

6.07B  Definitions for Division 6.1A

In this Division:

AFP means the Australian Federal Police established under the Australian Federal Police Act 1979.


background check of a person means:
   (a) a criminal records check of the person; and
   (b) unless a security assessment of the person has previously been conducted — a security assessment of the person conducted by ASIO.
Commonwealth authority means:
(a) a Commonwealth department; or
(b) a body established for a public purpose by or under a law of the Commonwealth.

conviction (of a person for an offence) has the meaning given by subsection 85ZM (1) of the Crimes Act 1914, but does not include:
(a) a spent conviction (within the meaning given by subsection 85ZM (2) of that Act); or
(b) a conviction for an offence of which, under a law relating to pardons or quashed convictions, the person is taken never to have been convicted.

DIMIA means the Department administered by the Minister who administers the Migration Act 1958.

disqualifying offence means an offence mentioned in item 1, 2 or 3 of Table 6.07C.

exempt person, in relation to a maritime security zone, means a person who:
(a) under the Act or these Regulations, is not required to properly display a valid MSIC in the zone; or
(b) under regulation 6.07HD or 6.07HE, is exempt from having to make an application for an MSIC during the MSIC implementation period, or part of the MSIC implementation period, for the zone.

holder, of an MSIC, means the person to whom it is issued.

issuing body means a person or body authorised to issue MSICs.

MSIC means maritime security identification card.

MSIC applicant means a person who has applied for the issue of an MSIC in accordance with regulation 6.08B.

MSIC implementation period means the period from the commencement of Subdivision 6.1A.1A until the end of 31 December 2006.

security assessment has the same meaning as in Part IV of the Australian Security Intelligence Organisation Act 1979.

sentence includes a suspended sentence.
Note 1 Under the definition of *conviction* in subsection 85ZM (1) of the *Crimes Act 1914*, somebody is also taken to have been convicted of an offence if he or she has been convicted of the offence but no conviction has been recorded, and if a court has taken the offence into account in sentencing him or her for another offence: see paragraphs 85ZM (1) (b) and (c) of that Act.

Note 2 Under Part VIIC of the *Crimes Act 1914*, if somebody receives a free and absolute pardon for an offence against a law of the Commonwealth or a Territory because he or she was wrongly convicted of the offence, he or she is taken for all purposes never to have been convicted — see section 85ZR of that Act.

Note 3 Under the *Crimes Act 1914*, a person need not disclose convictions that:
(a) have been quashed (see section 85ZT); or
(b) are spent (see section 85ZV).

Note 4 Convictions for disqualifying offences do not become spent for the purposes of an authority assessing whether to issue the convicted person with an MSIC — see the *Crimes Act 1914*, paragraph 85ZZH (k), and the *Crimes Regulations 1990*, regulation 8 and Schedule 4.

### 6.07C Meaning of maritime-security-relevant offence

In this division, a **maritime-security-relevant offence** means an offence of a kind mentioned in an item in Table 6.07C or a similar offence against a law of a State or Territory, or of any other country or part of a country.

#### Table 6.07C Maritime-security-relevant offences

<table>
<thead>
<tr>
<th>Item</th>
<th>Kind of offence</th>
</tr>
</thead>
</table>
| 1    | An offence mentioned in Chapter 5 of the *Criminal Code*.  
*Note* Offences for this item include treason, espionage and harming Australians. |
<p>| 2    | An offence involving the supply of goods (such as weapons or missiles) for a Weapons of Mass Destruction program as mentioned in the <em>Weapons of Mass Destruction (Prevention of Proliferation) Act 1995</em> |
| 3    | An offence involving the hijacking or destruction of an aircraft or vessel |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Kind of offence</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>An offence involving treachery, sabotage, sedition, inciting mutiny, unlawful drilling, or destroying or damaging Commonwealth property, mentioned in Part II of the <em>Crimes Act 1914</em></td>
</tr>
<tr>
<td>5</td>
<td>An offence involving interference with aviation, maritime transport infrastructure or an offshore facility, including carriage of dangerous goods on board an aircraft or ship, or endangering the security of an aerodrome, a port or an offshore facility</td>
</tr>
<tr>
<td>6</td>
<td>An identity offence involving counterfeiting or falsification of identity documents, or assuming another individual’s identity</td>
</tr>
<tr>
<td>7</td>
<td>Transnational crime involving money laundering, or another crime associated with organised crime or racketeering</td>
</tr>
<tr>
<td>8</td>
<td>People smuggling and related offences mentioned in Chapter 4, Division 73 of the <em>Criminal Code</em></td>
</tr>
<tr>
<td>9</td>
<td>An offence involving the importing, exporting, supply or production of weapons, explosives or a trafficable quantity of drugs.</td>
</tr>
</tbody>
</table>

**Note 1** A person convicted of an offence mentioned in item 1, 2 or 3 of Table 6.07C is disqualified from holding an MSIC, but, under regulation 6.08X, is entitled to seek reconsideration of the disqualification decision.

**Note 2** An issuing body must not issue an MSIC to a person who has been convicted of an offence mentioned in item 4, 5, 6, 7, 8 or 9 of Table 6.07C unless the Secretary, acting under regulation 6.08F, decides that the person is unlikely to constitute a security threat and approves the issue of an MSIC to the person.

**Note 3** Before 1 January 2007, a person who has been convicted of a disqualifying offence must not enter a maritime security zone: see regulations 6.07K and 6.08D.

### 6.07D Meaning of valid MSIC

(1) For this Division, an MSIC is *valid* if:

(a) it is issued in accordance with Subdivision 6.1A.4; and
(b) it is not expired or cancelled; and
(c) it is not altered or defaced (permanently or temporarily); and
(d) the person who shows or displays it is the person to whom it was issued.

(2) However, an MSIC issued to a person who changes his or her name ceases to be valid 1 month after the day on which the change is made.

6.07E Meaning of properly displaying

(1) For this Division, somebody is **properly displaying** an MSIC only if it is attached to his or her outer clothing:
   (a) above waist height; and
   (b) at the front or side of his or her body; and
   (c) with the whole front of the MSIC clearly visible.

(2) He or she is not **properly displaying** the MSIC if the photograph or anything else on it is obscured.

6.07F Meaning of operational need

For this Division, a person has **an operational need** to hold an MSIC if his or her occupation or business interests require, or will require, him or her to have unmonitored access to a maritime security zone at least once each year.

*Examples*

1 a person whose work takes him or her into a zone.
2 a representative of a maritime industry participant that has a business connection with the zone.
3 a representative of an employee association whose members work in the zone.
4 a representative of an industry association whose members include a maritime industry participant that has a connection with the zone.
5 a representative of an issuing body.

6.07G Kinds of identification document

(1) This regulation sets out the criteria that a document must meet to qualify as a primary, secondary or tertiary identification document for somebody.
(2) A document is a primary identification document for somebody if it is:
   (a) a certified copy (that is, a copy certified by a Registrar of Births or similar officer to be a correct copy) of the entry, in a register of births, of his or her birth; or
   (b) a copy (certified under section 44 of the Australian Citizenship Act 1948) of a citizenship certificate granted to him or her; or
   (c) a document issued to him or her under the law of another country that is evidence, under that law, that he or she is a citizen of that country; or
   (d) a passport issued to him or her.

(3) A document is a secondary identification document for somebody if:
   (a) it has on it a recent photograph of him or her, or his or her signature; and
   (b) it is:
       (i) a licence (for example, a driver’s licence) issued to him or her under a law of the Commonwealth or a State or Territory; or
       (ii) a government employee identification document issued to him or her; or
       (iii) an Australian student identification document issued to him or her; or
       (iv) a verifiable reference.

(4) In subregulation (3):

Australian student identification document means a card or document issued to a student at a tertiary education institution in Australia to identify him or her as a student at the institution.

government employee identification document means a document issued by or for the Commonwealth or a State or Territory to somebody employed by or for the Commonwealth or the State or Territory.

verifiable reference about somebody (the identified person) means a reference from:
   (a) a bank or similar financial institution; or
(b) somebody whose identity has been verified by means of:
   (i) 2 primary identification documents; or
   (ii) a primary identification document and a secondary identification document; or
   (iii) a primary identification document and 2 tertiary identification documents; or
(c) a referee acceptable to the person or body that requires the identification of the identified person;

that:
(d) identifies the identified person by name; and
(e) certifies that the person who signed the reference has known the identified person by that name for at least 12 months; and
(f) is signed by or for the referee and by the identified person.

(5) A document is a tertiary identification document for somebody if:
(a) it sets out his or her name and address; and
(b) it is:
   (i) a signed statement by his or her employer or former employer about that employment; or
   (ii) a copy (certified by a Registrar of Titles or similar officer to be a correct copy) of a record issued under a law about land titles; or
   (iii) a document issued by a rating authority from its records about land ownership or occupation; or
   (iv) a document issued by a bank or similar financial institution from its records about a mortgage or other security that he or she gave to the bank or institution; or
   (v) an extract from the electoral roll compiled by the Australian Electoral Commission; or
   (vi) a record issued under a law in force in Australia other than a law about land titles.
6.07H Authentication of certain foreign documents

(1) In this regulation:


(2) This regulation applies if a person presents to an issuing body, as an identification document, a document that is a public document for the purposes of the Hague Convention and was issued in a country (other than Australia) that is a Contracting State to that Convention.

(3) The body may require the person to have the authenticity of the document certified in accordance with that Convention.

\textit{Note} The authentication procedure involves the endorsement on, or attachment to, the document of a certificate in a standard form. Details of the procedure and any fee payable should be available from the embassy of the country in which the document was issued.

Subdivision 6.1A.1A MSIC implementation period

6.07HA Requirements during MSIC implementation period

(1) A person in a maritime security zone during the MSIC implementation period must be:

(a) the holder of a valid MSIC; or
(b) an MSIC applicant; or
(c) an exempt person.

(2) If a person in a maritime security zone is requested by a maritime security inspector to provide evidence that the person satisfies subregulation (1), the person has no more than 14 days after the day the inspector made the request (the \textit{request day}) to provide evidence to the Secretary that the person satisfied subregulation (1) on the request day.

\textit{Examples of evidence that a person satisfies subregulation 6.07HA (1)}:

1. A document from an issuing body or the person’s employer about the application.
2. A record of a telephone call made, or email sent, by the person to an issuing body.
3 A copy of the completed front page of the person’s application for an MSIC, a record of the person’s MSIC application number or the log-in details for the person’s electronic application for an MSIC.

(3) Subject to subregulation (2), a maritime security inspector may issue a warning notice to a person who does not comply with subregulation (1).

(4) A warning notice mentioned in subregulation (3) must:
   (a) be in a form approved by the Secretary; and
   (b) state:
       (i) the effect of subregulation (1); and
       (ii) that the person is not the holder of a valid MSIC, an MSIC applicant or an exempt person; and
   (c) direct the person to make an application for an MSIC in accordance with regulation 6.08B.

6.07HB MSIC implementation offence

(1) A person commits an offence if, on a day (the relevant day) during the MSIC implementation period, the person:
   (a) is in a maritime security zone; and
   (b) is not an MSIC applicant or the holder of a valid MSIC; and
   (c) is not an exempt person; and
   (d) has been issued with a warning notice under subregulation 6.07HA (3) more than 21 days before the relevant day.

   Penalty: 5 penalty units.

(2) Subregulation (1) does not apply to a person who, no more than 14 days after the relevant day, provides evidence to the Secretary that on the relevant day:
   (a) the person was an MSIC applicant; or
   (b) the person had reasonable grounds to believe that he or she would not have an operational need for unescorted or unmonitored access to a maritime security zone on or after 1 January 2007.
(3) For paragraph (2) (a), evidence may include any of the following:
   (a) a document from an issuing body or the person’s employer
       in respect of the application;
   (b) a statutory declaration by the person to the effect that an
       application has been made to an issuing body;
   (c) a copy of the completed front page of the application.

(4) For paragraph (2) (b), evidence may include a letter from, or
    statutory declaration by, a person responsible for the person
    being in the maritime security zone (a responsible person),
    stating or declaring as the case may be, that on the relevant day
    the responsible person believed that the person would not have
    an operational need for unescorted or unmonitored access to
    the zone on or after 1 January 2007.

(5) In this regulation:

   operational need, in relation to a person, means a need relating
   to the occupation or business interests of the person.

(6) An offence against subregulation (1) is an offence of strict
    liability.

   Note  For strict liability, see section 6.1 of the Criminal Code.

6.07HC Powers of maritime security inspectors during MSIC
implementation period

(1) If a person is in a maritime security zone during the MSIC
    implementation period and not properly displaying a valid
    MSIC, a maritime security inspector may direct the person to
    provide the inspector with evidence of 1 or more of the
    following:
    (a) the person’s identity and address;
    (b) if the person claims that he or she holds a valid MSIC —
        the valid MSIC;
    (c) if the person claims that he or she is an MSIC applicant —
        that the person is an MSIC applicant;
    (d) if the person claims that he or she is an exempt person —
        that the person is an exempt person;
(e) if the person claims that he or she does not require an MSIC — that the person does not require an MSIC.

(2) A maritime security inspector must not give a direction under subregulation (1) if the inspector knows the person is an exempt person in relation to the maritime security zone.

(3) Before directing the person to provide evidence for subregulation (1), the maritime security inspector must show the person the inspector’s identity card.

(4) A person must comply with a direction of a maritime security inspector under subregulation (1).

Penalty: 10 penalty units.

6.07HD Persons exempted from operation of regulation 6.07HB

(1) For paragraph (b) of the definition of exempt person in regulation 6.07B, a person is exempt from the requirement to be an MSIC applicant during the MSIC implementation period, or part of the period, if the person is in a maritime security zone in:

(a) a port mentioned in column 2 of an item in Table 6.07HD during the exemption period; or

(b) an on-board security zone established by the Secretary under subsection 110 (1) of the Act during the exemption period for that zone; or

(c) an offshore security zone established by the Secretary under subsection 113A (1) of the Act during the exemption period for that zone.

(2) In this regulation:

exemption period means:

(a) for a port — the period beginning on the day on which Subdivision 6.1A.1A commences, and ending at the end of the day specified for the port in column 3 of Table 6.07HD;
(b) for an on-board security zone — the period beginning on the day on which Subdivision 6.1A.1A commences, and ending at the end of 21 August 2006;

(c) for an offshore security zone — the period beginning on the day on which Subdivision 6.1A.1A commences, and ending at the end of 21 August 2006.

| Table 6.07HD  Port exemption period |
|-----------------|-----------------------------------|
| Item | Port                                           | End day of exemption period for a port |
| 1    | Port of Melbourne                           | 21 August 2006                     |
| 2    | Port Botany                                  | 21 August 2006                     |
| 3    | Port Jackson – Sydney Harbour                | 21 August 2006                     |
| 4    | Newcastle                                    | 21 August 2006                     |
| 5    | Brisbane                                     | 21 August 2006                     |
| 6    | Port Alma                                    | 21 August 2006                     |
| 7    | Gladstone                                    | 21 August 2006                     |
| 8    | Hay Point                                    | 21 August 2006                     |
| 9    | Townsville                                   | 21 August 2006                     |
| 10   | Cairns                                       | 21 August 2006                     |
| 11   | Darwin                                       | 21 August 2006                     |
| 12   | Adelaide                                     | 21 August 2006                     |
| 13   | Hobart                                       | 21 August 2006                     |
| 14   | Devonport                                    | 21 August 2006                     |
| 15   | Barrow Island                                | 21 August 2006                     |
| 16   | Broome                                       | 21 August 2006                     |
| 17   | Dampier                                      | 21 August 2006                     |
| 18   | Derby                                        | 21 August 2006                     |
| 19   | Fremantle                                     | 21 August 2006                     |
| 20   | Onslow (Airlie Island)                       | 21 August 2006                     |
| 21   | Onslow (Solar Salt)                          | 21 August 2006                     |
### Maritime Transport and Offshore Facilities Security Regulations 2003

**Item Port**

<table>
<thead>
<tr>
<th>Item</th>
<th>Port</th>
<th>End day of exemption period for a port</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Onslow (Thevenard Island and Saladin Marine Terminal)</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>23</td>
<td>Port Hedland</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>24</td>
<td>Port Walcott</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>25</td>
<td>Carnarvon (Useless Loop)</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>26</td>
<td>Carnarvon (Cape Cuvier)</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>27</td>
<td>Varanus Island</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>28</td>
<td>Wyndham</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>29</td>
<td>Yampi Sound (Cockatoo Island)</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>30</td>
<td>Eden</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>31</td>
<td>Norfolk Island</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>32</td>
<td>Port Kembla</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>33</td>
<td>Yamba</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>34</td>
<td>Geelong</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>35</td>
<td>Port of Hastings</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>36</td>
<td>Port of Corner Inlet and Port Albert</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>37</td>
<td>Portland</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>38</td>
<td>Geraldton</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>39</td>
<td>Albany</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>40</td>
<td>Bunbury</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>41</td>
<td>Esperance</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>42</td>
<td>Christmas Island</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>43</td>
<td>Cocos (Keeling) Island</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>44</td>
<td>Burnie</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>45</td>
<td>Grassy</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>46</td>
<td>Port Latta</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>47</td>
<td>Launceston</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>48</td>
<td>Spring Bay</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>Item</td>
<td>Port</td>
<td>End day of exemption period for a port</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>49</td>
<td>Stanley</td>
<td>21 August 2006</td>
</tr>
<tr>
<td>50</td>
<td>Bundaberg</td>
<td>4 September 2006</td>
</tr>
<tr>
<td>51</td>
<td>Karumba</td>
<td>4 September 2006</td>
</tr>
<tr>
<td>52</td>
<td>Abbot Point</td>
<td>4 September 2006</td>
</tr>
<tr>
<td>53</td>
<td>Lucinda</td>
<td>4 September 2006</td>
</tr>
<tr>
<td>54</td>
<td>Mackay</td>
<td>4 September 2006</td>
</tr>
<tr>
<td>55</td>
<td>Thursday Island</td>
<td>4 September 2006</td>
</tr>
<tr>
<td>56</td>
<td>Weipa</td>
<td>4 September 2006</td>
</tr>
<tr>
<td>57</td>
<td>Cape Flattery</td>
<td>4 September 2006</td>
</tr>
<tr>
<td>58</td>
<td>Mourilyan</td>
<td>4 September 2006</td>
</tr>
<tr>
<td>59</td>
<td>Bing Bong</td>
<td>11 September 2006</td>
</tr>
<tr>
<td>60</td>
<td>Gove</td>
<td>11 September 2006</td>
</tr>
<tr>
<td>61</td>
<td>Milner Bay</td>
<td>11 September 2006</td>
</tr>
<tr>
<td>62</td>
<td>Port Lincoln</td>
<td>11 September 2006</td>
</tr>
<tr>
<td>63</td>
<td>Port Pirie</td>
<td>11 September 2006</td>
</tr>
<tr>
<td>64</td>
<td>Whyalla</td>
<td>11 September 2006</td>
</tr>
<tr>
<td>65</td>
<td>Ardrossan</td>
<td>11 September 2006</td>
</tr>
<tr>
<td>66</td>
<td>Port Bonython</td>
<td>11 September 2006</td>
</tr>
<tr>
<td>67</td>
<td>Port Giles</td>
<td>11 September 2006</td>
</tr>
<tr>
<td>68</td>
<td>Thevenard, South Australia</td>
<td>11 September 2006</td>
</tr>
<tr>
<td>69</td>
<td>Wallaroo</td>
<td>11 September 2006</td>
</tr>
</tbody>
</table>
6.07HE Persons exempted by Secretary from operation of regulation 6.07HB

(1) For paragraph (b) of the definition of exempt person in regulation 6.07B, the Secretary may, on his or her own initiative, or on written application by a person or a maritime industry participant, give a person, or a class of persons, an exemption from the requirement to be an MSIC applicant during the MSIC implementation period, or part of the period, in a maritime security zone or zones.

(2) The exemption may be given subject to a condition or conditions.

(3) In deciding whether to give an exemption, the Secretary must consider:
   (a) the reasons the exemption is necessary; and
   (b) the likely effect of the exemption on the security of maritime transport or an offshore facility in the zone or zones; and
   (c) the period of the exemption; and
   (d) any other matter that the Secretary considers relevant.

(4) The exemption must specify the following:
   (a) the period in respect of which it is given;
   (b) if it is given in respect of a person — the name of the person;
   (c) if it is given in respect of a class of person — a description of the class;
   (d) if it is given subject to a condition or conditions — the condition or conditions;
   (e) the maritime security zone or zones in respect of which it is given.

(5) If the Secretary gives an exemption to a class of persons, the Secretary must publish a notice of the exemption in the Gazette.
Subdivision 6.1A.2 Display of MSICs

6.07I Definitions for Subdivision 6.1A.2

In this Subdivision:

escort means a person who escorts, or continuously monitors, another person in a maritime security zone.

Note Unless exempt, an escort must hold a valid MSIC: see regulation 6.07J.

visitor, to a maritime security zone, means a person who is entitled to be in the zone because he or she is being escorted or continuously monitored.

6.07J Requirement to display MSIC in maritime security zones

(1) A person commits an offence if:

(a) he or she is in a maritime security zone; and
(b) he or she fails to properly display a valid MSIC.

Penalty:

(c) for a first offence — 5 penalty units; or
(d) for a second offence within 2 years of an offence — 10 penalty units; or
(e) for a third or subsequent offence within 2 years of an offence — 20 penalty units.

(2) Subregulation (1) does not apply to:

(a) a visitor to the zone, if his or her escort:

(i) is displaying a valid MSIC; or

(ii) is carrying a valid MSIC but, under regulation 6.07M, is exempt from the requirement to display it; or

(iii) is exempt, under regulation 6.07M, from the requirement to carry a valid MSIC; or

(b) the holder of an identification document issued by an arm of the Defence Force who:

(i) is displaying his or her identification document; and
Regulation 6.07K

(ii) is in the zone as part of his or her duties for the Force; or
(c) a person who is in a private living area of a security regulated offshore facility.

(3) A contravention of subregulation (1) is an offence of strict liability.

(4) Subregulation (1) does not apply before 1 January 2007.

6.07K Person given disqualifying offence not to enter maritime security zone

(1) A person who has been given a disqualifying notice by the Secretary under regulation 6.08D must not enter a maritime security zone.

Penalty: 5 penalty units.

(2) Subregulation (1) does not apply to a person who is a visitor to a zone for the purpose of boarding or leaving a vessel as part of a recreational activity.

(3) A contravention of subregulation (1) is an offence of strict liability.

6.07L Offence — failure to properly escort visitor

(1) An escort is guilty of an offence if he or she fails to escort, or continuously monitor, a visitor in accordance with the procedures set out in the maritime security plan, ship security plan or offshore security plan of the maritime industry participant concerned.

Penalty: 5 penalty units.

(2) A contravention of subregulation (1) is an offence of strict liability.
6.07M Persons exempted by Secretary from requirement to hold, carry or display MSIC

(1) Despite regulation 6.07J, somebody to whom the Secretary has given an exemption under this regulation need not display an MSIC in a maritime security zone.

(2) Within 30 days after receiving an application, the Secretary must:
   (a) give or refuse the exemption; and
   (b) notify the person in writing of the decision and, if the decision is a refusal, the reasons for it.

(3) On the Secretary’s own initiative, or on written application by a person, the Secretary may give a person, or all persons in a specified class, exemption from the requirement, in 1 or more specified maritime security zones, to:
   (a) hold an MSIC; or
   (b) carry an MSIC; or
   (c) display an MSIC.

(4) Before giving or refusing an exemption, the Secretary must consider:
   (a) why the exemption is necessary; and
   (b) the likely effect of the proposed exemption on the security of maritime transport or an offshore facility in the zone; and
   (c) how long the proposed exemption will last, if it is given; and
   (d) anything else relevant that the Secretary knows about.

(5) The Secretary may give an exemption:
   (a) for a particular period and subject to a condition or conditions mentioned in the exemption; or
   (b) limited to a particular zone or part of a zone.

(6) If the Secretary gives an exemption to all persons in a specified class, the Secretary must publish a notice of the exemption in the *Gazette.*
6.07N Access by emergency personnel

(1) Nothing in this Division requires or authorises a maritime industry participant to prevent any of the following having access to any part of a maritime security zone:
(a) members of the Defence Force who are responding to an event or threat of unlawful interference with maritime transport or an offshore facility;
(b) ambulance, rescue or fire service officers who are responding to an emergency.

(2) A requirement of this Part to display an MSIC does not apply to a person referred to in paragraph (1) (a) or (b).

Subdivision 6.1A.3 MSIC issuing bodies

6.07O Application for authorisation to issue MSICs

(1) The following may apply, in writing, to the Secretary for authorisation as an issuing body:
(a) a maritime industry participant;
(b) a body representing participants;
(c) a body representing employees of participants;
(d) a Commonwealth authority.

Note Knowingly making a false or misleading statement in an application is an offence punishable by imprisonment for 12 months — see the Criminal Code, section 136.1.

(2) However, a participant may engage an agent to issue MSICs and the agent may apply to be an issuing body.

(3) An application must be accompanied by a statement setting out the applicant’s proposed MSIC plan.

(4) An applicant is entitled to perform the functions or exercise the powers of an issuing body only if the applicant’s MSIC plan is approved by the Secretary.
6.07P Decision on application

(1) If the Secretary needs more information to deal with an application under regulation 6.07O, the Secretary may ask the applicant, in writing, to provide the information.

(2) Before the end of 30 days after receiving an application (or, if the Secretary asks for more information under subregulation (1), before the end of 30 days after receiving the information), the Secretary must:
   (a) approve, or refuse to approve, the applicant’s proposed MSIC plan; and
   (b) authorise, or refuse to authorise, the applicant as an issuing body; and
   (c) notify the body in writing of the decision and, if the decision is a refusal, the reasons for the decision.

Note Section 27A of the Administrative Appeals Tribunal Act 1975 requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person’s right to have the notice reviewed.

(3) If the Secretary has not authorised, or refused to authorise the applicant as an issuing body within the period allowed by subregulation (2), the Secretary is taken to have refused to authorise the applicant as an issuing body.

(4) The Secretary must not authorise the applicant as an issuing body unless the Secretary is satisfied that:
   (a) the applicant’s MSIC plan is apparently adequate to give effect to the proposed plan’s purposes; and
   (b) authorising the applicant as an issuing body would not be likely to be a threat to the security of maritime transport or an offshore facility.

(5) The Secretary may authorise an applicant as an issuing body subject to a condition set out in the instrument of authorisation.

6.07Q What an MSIC plan is

(1) An MSIC plan sets out procedures to be followed for the following purposes:
   (a) the issue and production of MSICs;
(b) the design, distribution and storage of sample MSICs for training purposes, if the issuing body proposes to issue such MSICs;

(c) the safekeeping, secure transport and disposal of MSICs and associated equipment;

(d) the recovery and secure destruction of issued MSICs that are no longer required;

(e) the security of records in relation to applicants for MSICs;

(f) lost, destroyed or stolen MSICs;

(g) ensuring that MSICs are returned to issuing bodies when they are no longer required.

(2) An MSIC plan must also set out the procedures that will be followed if the applicant is authorised as an issuing body and the authorisation is later revoked, including procedures to ensure that information about applications for MSICs, and holders of MSICs, is appropriately preserved.

Note An applicant for authorisation as an issuing body must provide with its application a statement of its proposed MSIC plan — see regulation 6.07O.

6.07R Issuing body to give effect to MSIC plan

(1) An issuing body must not fail to give effect to its MSIC plan.

Penalty: 50 penalty units.

(2) Without limiting subregulation (1), an issuing body fails to give effect to its MSIC plan if it:

(a) fails to do something that its MSIC plan requires that it do;

or

(b) does something that its MSIC plan requires that it not do;

or

(c) does something that its MSIC plan requires that it do, but does so in a way that contravenes the plan.

(3) A contravention of subregulation (1) is an offence of strict liability.
(4) However, an issuing body may apply, in writing, to the Secretary for exemption from giving effect to its MSIC plan in a particular case or respect.

(5) If the Secretary needs more information to deal with an application, the Secretary may ask the applicant, in writing, to provide the information.

(6) Within 30 days after receiving an application (or, if the Secretary asks for more information under subregulation (5), within 30 days after receiving the information), the Secretary must:

(a) grant or refuse the exemption; and
(b) notify the body in writing of the decision and, if the decision is a refusal, the reasons for the decision.

Note Section 27A of the Administrative Appeals Tribunal Act 1975 requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person’s right to have the notice reviewed.

(7) If the Secretary has not approved, or refused to approve, the exemption within the period allowed by subregulation (6), the Secretary is taken to have refused to approve the exemption.

(8) The Secretary may also grant, on his or her own initiative, an issuing body a written exemption from giving effect to its MSIC plan in a particular case or respect.

(9) Before granting or refusing an exemption under this regulation, the Secretary must consider:

(a) the justification for the proposed exemption; and
(b) the likely effect of the proposed exemption on each of the plan purposes; and
(c) how long the proposed exemption will be for, if it is granted; and
(d) anything else relevant that the Secretary knows about.

(10) The Secretary may grant an exemption for a particular period and subject to a condition mentioned in the exemption.
Part 6 Maritime security zones
Division 6.1A Control of maritime security zones

Regulation 6.07S

6.07S Direction to vary MSIC plan

(1) If an issuing body’s MSIC plan is not adequate to give effect, in all circumstances, to any 1 or more of the plan purposes, the Secretary may direct the body, in writing, to vary the plan.

(2) The Secretary must not give such a direction in relation to a plan purpose unless the Secretary is satisfied that the variation is appropriate to make the plan adequate for that purpose.

(3) A direction must:
   (a) indicate the variation needed; and
   (b) state the time within which the issuing body must submit an appropriately varied plan to the Secretary.

(4) An issuing body must comply with such a direction.

Note Regulation 6.07W provides for the revocation of the authorisation of a body that does not comply with a direction.

6.07T Variation of MSIC plan by issuing body

(1) An issuing body may:
   (a) review its MSIC plan at any time; and
   (b) submit a written proposed variation of the plan to the Secretary for approval.

(2) If the Secretary needs more information to deal with a proposed variation, the Secretary may ask the body, in writing, to provide the information.

(3) Before the end of 30 days after receiving the proposed variation (or, if the Secretary asks for more information under subregulation (2)), before the end of 30 days after receiving the information), the Secretary must:
   (a) approve or refuse to approve the variation; and
   (b) notify the body in writing of the decision and, if the decision is a refusal, the reasons for the decision.

Note Section 27A of the Administrative Appeals Tribunal Act 1975 requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person’s right to have the notice reviewed.
(4) If the Secretary has not approved, or refused to approve, the variation within the period allowed by subregulation (3), the Secretary is taken to have refused to approve the variation.

(5) The Secretary must approve the variation if the plan, as varied, will give effect to the plan purposes.

6.07U Inspection of issuing bodies' MSIC plan and records

(1) An issuing body must:
   (a) keep a copy of its MSIC plan or any variation to the plan for at least 7 years after the day on which the plan is approved or varied; and
   (b) keep any record relating to how the body gives effect to its MSIC plan for at least 7 years after the day on which it is made.

(2) An issuing body must allow a maritime security inspector to inspect the plan and records kept for subregulation (1) on request, subject to reasonable notice.

6.07V Issuing bodies’ staff

(1) An issuing body other than a Commonwealth authority must not allow a person to be directly involved in the issue of MSICs unless he or she is able to satisfy the security-relevant criteria for the issue of an MSIC.

Penalty: 20 penalty units.

(2) A Commonwealth authority that is an issuing body must not allow a person to be directly involved in the issue of MSICs unless he or she is able to satisfy the security-relevant criteria for the issue of an MSIC.

(3) Despite subregulations (1) and (2) the Secretary may approve the involvement of a person in the issue of MSICs if:
   (a) a security assessment of the person is qualified; but
   (b) the Secretary is satisfied that the involvement of the person in the issue of MSICs would not constitute a threat to the security of maritime transport or an offshore facility.
(4) For subregulations (1) and (2), a person satisfies the security-relevant criteria for the issue of an MSIC if he or she is able to satisfy the criteria for the issue of an MSIC set out in paragraphs 6.08C (1) (b), (c), (d) and (e).

6.07W Revocation of authorisation for cause

(1) The Secretary must revoke an issuing body’s authorisation as an issuing body if in the opinion of the Secretary:
   (a) the body’s MSIC plan is apparently no longer adequate to give effect to a plan purpose and it is unlikely that a direction under regulation 6.07S will make the plan adequate for that purpose; or
   (b) allowing the body’s authorisation to continue would be likely to be a significant threat to the security of maritime transport or an offshore facility; or
   (c) the body does not comply with a direction of the Secretary under regulation 6.07S.

(2) The Secretary may revoke the authorisation of an issuing body if the body contravenes:
   (a) a condition of its authorisation; or
   (b) its MSIC plan.

(3) For subregulation (2), the Secretary must consider:
   (a) the kind and seriousness of the contravention; and
   (b) whether the issuing body has previously contravened a condition of its authorisation or its MSIC plan.

(4) As soon as practicable after revoking the authorisation of a body under this regulation, the Secretary must notify the body in writing of the revocation and the reasons for the revocation.

   Note Section 27A of the Administrative Appeals Tribunal Act 1975 requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person’s right to have the notice reviewed.

(5) The revocation takes effect when written notice of the revocation is given to the body.
6.07X Revocation of authorisation at request of issuing body

(1) The Secretary must revoke the authorisation of a body as an issuing body if the body asks the Secretary, in writing, to do so.

(2) A revocation under subregulation (1) takes effect when the request was made.

6.07Y Re-applying for authorisation

A body whose authorisation is revoked may apply under regulation 6.07O for a new authorisation.

6.07Z What happens if issuing body no longer able to issue MSICs

(1) This regulation applies if:

(a) the authorisation of an issuing body (the original issuing body) is revoked; or

(b) the body ceases to exist; or

(c) for any other reason, the body no longer performs the functions or exercises the powers of an issuing body.

(2) The Secretary may authorise, in writing, another person to perform the functions, and exercise the powers, of the original issuing body (other than functions and powers relating to the documents mentioned in paragraph (5) (a)) in relation to MSICs issued by that body.

(3) An MSIC issued by the original issuing body that is in force at the time of such an authorisation is not affected by:

(a) the body having ceased to exist; or

(b) the new authorisation.

(4) The person authorised under subregulation (2) is taken to be the issuing body for the MSIC, but is not responsible for the actions of the original issuing body in relation to the MSIC before the authorisation.
Part 6  Maritime security zones
Division 6.1A  Control of maritime security zones

Regulation 6.08A

(5) An authorisation:
(a) is subject to the condition that any documents used to decide about the eligibility of a person for an MSIC are to be held by the Secretary; and
(b) may be subject to another condition specified in it.

Subdivision 6.1A.4  MSICs: issue, expiry and cancellation

6.08A  Meaning of adverse criminal record
For this Subdivision, a person has an adverse criminal record if he or she has been convicted of a maritime-security-relevant offence and sentenced to imprisonment (including periodic detention, home-based detention, and detention until the rising of the court, but not including a sentence of community service).

Note  For the meaning of maritime-security-relevant offence, see regulation 6.07C.

6.08B  MSICs — application for issue
(1) A person may, in writing, apply to an issuing body for the issue of an MSIC if he or she has an operational need to hold an MSIC.

(2) An applicant who has turned 18 must prepare a signed form of consent to background checking of the applicant and:
(a) if applying before 1 January 2007 — send the form to the AFP; or
(b) if applying on or after 1 January 2007 — include the form with the application.

6.08C  MSICs — issue
(1) An issuing body may issue an MSIC to a person only if:
(a) the person has an operational need to hold an MSIC; and
(b) the person has verified his or her identity by showing the issuing body:
   (i) a primary identification document; and
(ii) either:
   (A) a secondary identification document; or
   (B) 2 tertiary identification documents; and
(c) either:
   (i) has shown the issuing body a document that is evidence that the person is an Australian citizen (for example, his or her Australian birth certificate, Australian passport or Australian naturalisation certificate); or
   (ii) the issuing body is satisfied that he or she holds a visa entitling him or her to work in Australia; and
(d) the issuing body has been notified in writing that a security assessment of the person has been made, and:
   (i) the assessment was not adverse; or
   (ii) if the assessment was qualified — the issuing body has not been directed by the Secretary under subregulation 6.08H (2) not to issue an MSIC to the person; and
(e) the issuing body has been notified in writing that a criminal records check of the person has been made, and:
   (i) the check shows that the person does not have an adverse criminal record; or
   (ii) if the check shows that the person has an adverse criminal record — the Secretary has approved an application to issue an MSIC to the person under paragraph 6.08F (3) (a).

Penalty: 50 penalty units.

(2) For subparagraphs (1) (e) (i) and (ii):
   (a) from 1 October 2005 to the end of 31 December 2006 — the Secretary; or
   (b) on and after 1 January 2007 — the issuing body;
       must decide whether the criminal records check shows that the person has an adverse criminal record.

(3) An offence against subregulation (1) is an offence of strict liability.
(4) In the case of a person who is under 18, the issuing body may issue an MSIC to him or her despite paragraphs (1) (d) and (e) if he or she meets the criteria in paragraphs (1) (a), (b) and (c).

Note An MSIC issued under subregulation (3) ceases to be valid 6 months after the holder turns 18: see paragraph 6.08I (2) (a).

(5) If a person’s MSIC is cancelled at his or her request under regulation 6.08N and, less than 12 months after the cancellation, the person:
   (a) has an operational need to hold an MSIC; and
   (b) gives an issuing authority a statutory declaration stating that, since the cancellation, no relevant circumstance of the person has changed;
the issuing body may issue the MSIC to him or her despite anything in subregulation (1).

(6) An issuing body may issue an MSIC subject to a condition, but must notify the holder in writing what the condition is.

Example
A condition that background checking of the holder is carried out more frequently than required by these Regulations.

(7) An issuing body may issue MSICs only in accordance with its MSIC plan.

6.08D Issue of disqualifying offence notice

(1) This regulation applies if, before 1 January 2007, the background check of an applicant for an MSIC reveals that:
   (a) he or she has been convicted of a disqualifying offence; or
   (b) the security assessment of the person is adverse and is not a qualified security assessment.

(2) The Secretary must send the person a notice in writing (a disqualifying notice) that informs the person about the results of the background check and the effect of regulation 6.07K in relation to the person.
6.08E Issue of MSICs to ASIC holders

An issuing body may issue an MSIC to a person without verifying that the person has satisfied the criteria set out in subregulation 6.08C (1) if the person:

(a) holds an ASIC issued under the *Aviation Transport Security Regulations 2005*; and

(b) has an operational need for an MSIC.

*Note* The MSIC expires on the same day as the ASIC: see paragraph 6.08I (2) (c).

6.08F MSICs — Secretary’s approval of issue in certain cases

(1) If:

(a) a person is not eligible to be issued an MSIC only because he or she has an adverse criminal record; and

(b) he or she has not been convicted of a disqualifying offence;

an issuing body or the applicant may apply to the Secretary, in writing, for approval to issue an MSIC to the person.

(2) If the Secretary needs more information to deal with an application, the Secretary may ask the issuing body or applicant, in writing, to provide the information.

(3) Within 30 days after receiving an application (or, if the Secretary has asked for information under subregulation (2), after receiving the information), the Secretary must:

(a) approve, or refuse to approve, in writing, the issuing of the MSIC; and

(b) notify the body, or applicant, in writing of the decision and, if the decision is a refusal, notify the applicant of the reasons for the decision.

*Note* Section 27A of the *Administrative Appeals Tribunal Act 1975* requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person’s right to have the notice reviewed.
Regulation 6.08G

(4) If the Secretary has not approved, or refused to approve, the issue of the MSIC within the period allowed by subregulation (3), the Secretary is taken to have refused to approve the issue of the MSIC.

(5) Before approving or refusing to approve the issue of the MSIC to a person who is not eligible to be issued an MSIC only because, under paragraph 6.08C (1) (e), the person’s criminal record prevents him or her being issued with an MSIC, the Secretary must decide whether the person constitutes a threat to the security of maritime transport or an offshore facility by considering:

(a) the nature of the offence the person was convicted of; and
(b) the length of the term of imprisonment imposed on him or her; and
(c) if he or she has served the term, or part of the term — how long it is, and his or her conduct and employment history, since he or she did so; and
(d) if the whole of the sentence was suspended — how long the sentence is, and his or her conduct and employment history, since the sentence was imposed; and
(e) anything else relevant that the Secretary knows about.

(6) The Secretary may give an approval subject to a condition, but must notify the issuing body in writing what the condition is.

Example
A condition that background checking is conducted at specified intervals.

6.08G Report to Secretary of refusal to issue MSICs in certain cases

(1) If, on or after 1 January 2007, an issuing body refuses to issue an MSIC to an applicant because the applicant fails to satisfy a criterion in paragraph 6.08C (1) (c) or (e), the issuing body must, within 7 days of the decision, give the Secretary a written report that sets out:

(a) the applicant’s name, address and date of birth; and
(b) the reasons for the refusal.
(2) The Secretary may pass the information mentioned in paragraph (1) (a) on to other issuing bodies if he or she thinks that doing so will help to prevent unlawful interference with maritime transport or an offshore facility.

6.08H Persons the subject of adverse or qualified security assessments

(1) If a security assessment of a person is an adverse security assessment, the Secretary must direct an issuing body that proposes to issue an MSIC to the person that the MSIC is not to be issued.

(2) The Secretary may direct an issuing body not to issue an MSIC to a person if, on the basis of a security assessment of the person that is a qualified security assessment, the Secretary is satisfied that the holding of an MSIC by the person would constitute a threat to the security of maritime transport or an offshore facility.

(3) A direction under subregulation (1) or (2) must be in writing.

(4) An issuing body must not issue an MSIC to a person in contravention of a direction under subregulation (1) or (2).

Penalty: 20 penalty units.

Note If an adverse or qualified security assessment about a person is provided to a Commonwealth authority, the authority must notify the person in writing within 14 days (including a copy of the assessment) and must notify him or her how to apply to the Administrative Appeals Tribunal for review of the assessment — see the Australian Security Intelligence Organisation Act 1979, section 38.

6.08I MSICs — period of issue and expiry

(1) Unless earlier cancelled, an MSIC expires 5 years after the day when the relevant criminal records check conducted by the AFP is completed.

(2) However:
   (a) an MSIC issued to a person under 18 in reliance on subregulation 6.08C (3) must expire no later than 6 months after the person’s 18th birthday; and
(b) an MSIC issued to a person who is entitled to remain in Australia because he or she holds a visa must expire no later than the day on which the person’s visa expires; and

(c) an MSIC issued under regulation 6.08E must expire on the same day as the ASIC mentioned in paragraph 6.08E (a).

6.08J Form of MSICs other than temporary MSICs

(1) This regulation does not apply to a temporary MSIC.

Note For details about temporary MSICs, see regulation 6.08K.

(2) The form of an MSIC is as follows:

(3) An MSIC must comply with the following requirements:

(a) the dimensions of the MSIC, and of each of its parts, must be as shown in the diagram in subregulation (2);
(b) where the diagram indicates a particular colour, type-face or type size, that colour, type-face or type size must be used;

(c) the photograph of the holder must be a recent (that is, taken within 6 months before the issue of the MSIC) photograph of the holder, showing the holder’s full face and his or her head and shoulders;

(d) the photograph must be protected against tampering by a method that is approved by the Secretary and identified in a notice published in the Gazette;

(e) subject to subregulation (3B), the first name and surname must be those that the holder normally uses;

(f) the number must be unique among MSICs issued by that issuing body and include the issuing body identifier as directed by, or agreed with, the Secretary;

(h) the expiry date must be expressed as day abbreviated month year, where abbreviated month means the first 3 letters of the name of the month of expiry.

(3A) On an MSIC, the holder’s name must appear:

(a) if each word in the name consists of 10 characters or less — in 20 point Arial bold; or

(b) if a word in the name consists of more than 10 characters — in Arial bold of a size, being no less than 12 point, that results in the longest word in the name being reproduced as close to 32 mm wide as is practicable.

(3B) However, if setting out the holder’s name on an MSIC in accordance with subregulation (3A) would result in the name not being easily readable, the Secretary may approve, in writing, the issue of an MSIC with the holder’s name set out in Arial bold in another way.

(4) An MSIC that is issued to a law enforcement officer or an officer or employee of ASIO may bear the holder’s name on the back of the MSIC.

(5) The Secretary may approve the issue of an MSIC showing the holder’s name on the back if the Secretary is satisfied that having the holder’s name on the front would put the holder’s personal security at risk.
(6) An issuing body must not issue an MSIC that does not comply with subregulations (2), (3), (4) and (5).

Penalty: 50 penalty units.

(7) An offence under subregulation (6) is an offence of strict liability.

Note 1 For strict liability, see section 6.1 of the Criminal Code.

Note 2 National Privacy Principle 7, set out in Schedule 3 to the Privacy Act 1988, restricts the uses to which an identifier of an individual can be put.

6.08K Temporary MSICs

(1) A temporary MSIC may be issued to a person by:
(a) an issuing body; or
(b) if it acts in accordance with its maritime security plan, ship security plan or offshore security plan — a maritime industry participant;

if:
(c) the person is the holder of another MSIC and has forgotten the other MSIC, or it has been lost, stolen or destroyed; and
(d) the issuing body or participant is satisfied about the identity of the person.

(2) The issuing body or participant may issue an MSIC that is valid only for a specified period.

6.08L Issue of replacement MSICs

(1) An issuing body may issue a replacement MSIC to the holder of another MSIC if he or she has lost the other MSIC, or it has been stolen or destroyed, and:
(a) he or she has made a statutory declaration setting out the circumstances of the loss, theft or destruction; or
(b) if the other MSIC has been stolen — he or she has given the issuing body a copy of a police report, or other information issued by the police, regarding the theft.
(2) If the holder of an MSIC changes his or her name, an issuing body may issue a replacement MSIC to the holder after:
   (a) the holder provides written evidence of the change; and
   (b) the issuing body notifies ASIO of the change of name and ASIO acknowledges receipt of the notification.

(3) A replacement MSIC must expire no later than the earlier MSIC would have expired.

6.08M Cancellation of MSICs

(1) An issuing body must immediately cancel an MSIC issued by the body if:
   (a) the body finds out that the MSIC was not issued in accordance with the body’s MSIC plan; or
   (b) the Secretary finds out that the MSIC was not issued in accordance with the body’s MSIC plan and notifies the issuing body in writing; or
   (c) the Secretary has notified the issuing body in writing that a security assessment of the holder was adverse; or
   (d) the body finds out that the holder is not entitled to work in Australia; or
   (e) the body finds out that the holder has been convicted of a disqualifying offence; or
   (f) the holder no longer has an operational need to hold an MSIC; or
   (g) the body finds out that, for a continuous period of 12 months, the holder has not had an operational need to hold an MSIC.

   Note for paragraph (1) (e) See regulation 6.07B for the meaning of disqualifying offence.

(2) As soon as practicable after an issuing body cancels an MSIC under subregulation (1), the body must notify the holder, in writing, that the MSIC has been cancelled and the reasons for the cancellation.

   Note Section 27A of the Administrative Appeals Tribunal Act 1975 requires a person who makes a reviewable decision to give a person whose interests are affected by the decision notice of the making of the decision and of the person’s right to have the notice reviewed.
(3) A cancellation under subregulation (1) takes effect when the holder is notified of it in writing.

6.08N Cancellation of MSICs at holder’s request

(1) An issuing body must cancel an MSIC issued by the body if the holder of the MSIC asks the body to cancel it.

(2) A cancellation under subregulation (1) takes effect when the MSIC is returned to the issuing body.

6.08O Report to Secretary of cancellation of MSICs in certain cases

(1) If an issuing body cancels an MSIC on the basis of paragraph 6.08M (1) (c), (d), or (e), the issuing body must, within 7 days of the decision, give the Secretary a written report that sets out:
   (a) the holder’s name, address and date of birth; and
   (b) the reasons for the cancellation.

(2) The Secretary may pass the information mentioned in paragraph (1) (a) on to other issuing bodies if he or she thinks that doing so will help to prevent unlawful interference with maritime transport or an offshore facility.

6.08P Return of MSICs that have expired etc

(1) The holder of an MSIC must return it to an issuing body 30 days or less after:
   (a) the MSIC expires; or
   (b) the holder is notified that it has been cancelled; or
   (c) the MSIC has been damaged, altered or defaced (permanently or temporarily).

   Penalty: 10 penalty units.

(2) A contravention of subregulation (1) is an offence of strict liability.

6.08Q Holder no longer needing MSIC

(1) The holder of an MSIC is guilty of an offence if:
Maritime Transport and Offshore Facilities Security Regulations 2003

Regulation 6.08S

(a) he or she becomes aware of circumstances that will result in him or her not having an operational need to hold the MSIC for 12 months; and
(b) he or she fails to return it to an issuing body within 30 days of becoming aware of the circumstances.

Penalty: 5 penalty units.

(2) Strict liability applies to paragraph (1) (b).

6.08R Notification of lost etc MSICs

(1) The holder of an MSIC commits an offence if:
(a) the MSIC has been lost, stolen or destroyed; and
(b) the holder of the MSIC knows about the loss, theft or destruction; and
(c) he or she does not:
   (i) make a report, in the form of a statutory declaration, of the loss to the issuing body that issued the MSIC within 7 days of becoming aware of the loss, theft or destruction; or
   (ii) if the MSIC was stolen — give the issuing body a copy of a police report, or other information issued by the police, regarding the theft, within 7 days of becoming aware of the theft.

Penalty: 10 penalty units.

(2) Strict liability applies to paragraph (1) (c).

(3) However, subregulation (1) does not apply if the MSIC has been destroyed by the issuing body that issued it.

Subdivision 6.1A.5 Powers of security officers in relation to MSICs

6.08S Directions to show valid MSICs or other identification

(1) In this regulation:

exempt person, in relation to a part of a maritime security zone, means somebody who, under the Act or these
Regulation 6.08T

Regulations, is not required to properly display a valid MSIC in that part of that zone.

security officer means:
(a) a law enforcement officer; or
(b) a maritime security inspector.

(2) If a person is in a part of a maritime security zone and apparently not properly displaying a valid MSIC, a security officer may (unless he or she knows the person to be an exempt person in relation to that part of the zone) direct the person to show him or her a valid MSIC, or identification that establishes that the person is an exempt person.

(3) Before directing the person to do so, the security officer must show the person:
(a) the officer’s identity card; or
(b) another appropriate form of identification.

(4) A person must comply with a direction of a security officer under subregulation (2).

Penalty: 10 penalty units.

Subdivision 6.1A.6 Record-keeping

6.08T Register of MSICs

(1) An issuing body must keep a register in accordance with this regulation.

(2) The register must contain the following details of each MSIC issued by the body to a person:
(a) his or her name and telephone number (if any);
(b) a copy of the photograph that appears on his or her MSIC;
(c) subject to subregulation (3), his or her residential address;
(d) the general reason that he or she has an operational need to hold an MSIC;
(e) the documents used to decide about his or her eligibility for an MSIC;
(f) the date of the beginning of the current period during which he or she has continuously held an MSIC;

(g) the unique number of the MSIC;

(h) its date of issue;

(i) its date of expiry;

(j) if applicable, the date on which it was cancelled;

(k) if applicable, the date or dates on which it was reported lost, stolen or destroyed.

(3) The register need not contain the residential address of an MSIC holder who is:

(a) a law enforcement officer; or

(b) an officer or employee of ASIO; or

(c) an employee of a Commonwealth authority.

6.08U Other records

(1) An issuing body must maintain records that are sufficient to demonstrate that it has complied with its MSIC plan.

(2) The body must retain the record of issue of an MSIC to a person for at least 7 years after the creation of the record.

(3) The records may be kept by means of a computer or in any other form that can be conveniently audited.

(4) The issuing body must hold the records at its office.

(5) The issuing body must allow a maritime security inspector to inspect the records on request, subject to reasonable notice.

6.08V Annual reporting

An issuing body must report to the Secretary in writing, within 1 month after the end of each financial year:

(a) the total number of MSICs issued by the body; and

(b) the number of MSICs issued by the body that have not expired and have not been cancelled; and

(c) the number of MSICs issued by the body that have expired or been cancelled but have not been returned to the body; and
(d) the number of MSICs issued by the body that were
cancelled in the financial year to which the report relates;
and
(e) the number of MSICs issued by the body that expired in
that financial year.

Penalty: 20 penalty units.

Subdivision 6.1A.7 Review of decisions

6.08W Definitions

In this Subdivision:

AAT Act means the Administrative Appeals Tribunal Act 1975.
decision has the same meaning as in the AAT Act.
Tribunal means the Administrative Appeals Tribunal.

6.08X Reconsideration of decisions in relation to MSICs
and related matters

Decisions in relation to issuing bodies

(1) Application may be made to the Secretary for reconsideration
of a decision of the Secretary:
(a) to refuse to authorise a person as an issuing body; or
(b) to impose a condition on an issuing body; or
(c) to direct an issuing body to vary its MSIC plan; or
(d) to refuse to approve a variation of an issuing body’s MSIC
plan; or
(e) to refuse to exempt an issuing body from giving effect to
its MSIC plan in a particular case or respect; or
(f) to impose a condition on an exemption; or
(g) to revoke an issuing body’s authorisation.

Decisions in relation to adverse maritime security status

(2) Application may be made to the Secretary for reconsideration
of a decision of the Secretary that on the basis of a qualified
security assessment, a person has an adverse maritime security status.

Decisions in relation to issue and cancellation of MSICs

(3) Application may be made to the Secretary for:
(a) reconsideration of a decision of the Secretary to:
   (i) refuse to authorise the issue of an MSIC; or
   (ii) impose a condition on an MSIC; or
(b) review of a decision of an issuing body to:
   (i) refuse to issue an MSIC to somebody; or
   (ii) issue an MSIC subject to a condition; or
   (iii) cancel an MSIC.

Decisions in relation to wearing and use of MSICs

(4) Application may be made to the Secretary for reconsideration of a decision of the Secretary:
(a) to refuse to exempt somebody from displaying a valid MSIC in a maritime security zone, or part of such an area; or
(b) to impose a condition on such an exemption.

Decisions in relation to the substituted exercise of the powers of an issuing body

(5) Application may be made to the Secretary for reconsideration of a decision of the Secretary:
(a) to authorise, or refuse to authorise, a person to perform the functions, or exercise the powers, of an issuing body; or
(b) to authorise a person to perform the functions or exercise the powers of an issuing body subject to a condition.

Decisions in relation to issue of disqualifying notice

(6) Application may be made to the Secretary for reconsideration of a decision of the Secretary to issue a disqualifying notice under regulation 6.07K.
6.08Y If Secretary makes no decision

If person applies to the Secretary under regulation 6.08X for reconsideration or review of a decision and, 30 days after making the application, the Secretary has not notified his or her decision about the application to the applicant, the Secretary is taken to have refused to vary the original decision.

6.08Z AAT review of Secretary’s decisions

Application may be made under the AAT Act to the Tribunal for review of a decision made by the Secretary as a result of an application under regulation 6.08X.

Subdivision 6.1A.8 Miscellaneous

6.09A Cost recovery

An issuing body may recover the reasonable costs of the issue of an MSIC from the person who asks the body to issue the MSIC.

Division 6.2 Port security zones

Subdivision 6.2.1 General

6.20 Types of port security zones

For subsection 103 (1) of the Act, the following are prescribed as the types of port security zones that the Secretary may establish within a security regulated port:

(a) land-side restricted zones;
(b) cleared zones;
(c) water-side restricted zones.

6.25 Security barriers

(1) A fence, free standing wall, building or other similar object, or a series of objects such as trees, booms, marker buoys and
other similar objects, may constitute a *security barrier* if the object or series of objects:
(a) clearly defines the boundary of a maritime security zone; and
(b) deters unauthorised access into the zone.

(2) A security barrier for a land-side restricted zone or a cleared zone must:
(a) deter and deny unauthorised access to the zone; and
(b) allow detection of unauthorised access to the zone; and
(c) have access control points to permit authorised access, being access control points that do not present less of a barrier to unauthorised access than the surrounding parts of the security barrier; and
(d) be subject to regular patrols, surveillance or other measures that allow inspection of the security barrier for damage, and that detect and deter unauthorised access.

**Subdivision 6.2.2 Land-side restricted zones**

**6.30 Identification of zones**

(1) The boundaries of a land-side restricted zone must be clearly identifiable and defined by means of a security barrier.

(2) Persons who are in or in the vicinity of the security regulated port in which a land-side restricted zone is established must be informed that:
(a) access to the zone is controlled; and
(b) any unauthorised entry into the zone is an offence under these Regulations.

**6.33 Duties of port operator**

(1) A port operator must monitor and control access to any land-side restricted zone in the security regulated port in which the zone is established.

Penalty: 200 penalty units.
(2) An offence against subregulation (1) is an offence of strict liability.

**6.35 Duties of port facility operator**

(1) A port facility operator must monitor and control access to any land-side restricted zone within the boundaries of the port facility.

Penalty: 200 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

**6.40 Duties of port service provider**

(1) A port service provider must monitor and control access to any port security zone within the boundaries of the area under the control of the provider.

Penalty: 200 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

**6.45 Offences — unauthorised entry**

(1) A person must not enter or remain in a land-side restricted zone unless authorised to do so by:

(a) the port operator for the security regulated port; or
(b) the port facility operator for the port facility; or
(c) the port service provider that controls the land; in which the zone is established.

Penalty: 50 penalty units.

(2) A person must not take a vehicle or thing into, or leave a vehicle or thing in, a land-side restricted zone unless authorised to do so by:

(a) the port operator for the security regulated port; or
(b) the port facility operator for the port facility; or
(c) the port service provider that controls the land; in which the zone is established.

Penalty: 50 penalty units.

(3) An offence against subregulation (1) or (2) is an offence of strict liability.

**Subdivision 6.2.3 Cleared zones**

**6.50 Duties of port facility operator**

(1) Immediately after the Secretary gives notice of the establishment of a cleared zone (but before the zone comes into force), the port facility operator for the port facility in which the zone is established must ensure that the zone is inspected for unauthorised persons, goods (including weapons and prohibited items), vehicles and vessels.

(2) A port facility operator must ensure that persons and goods are screened and cleared in accordance with these Regulations before they are allowed to enter and remain in any cleared zone established in the port facility.

**6.55 Identification of zones**

(1) The boundaries of a cleared zone must be clearly identifiable and defined by means of a security barrier.

(2) Persons who are in or in the vicinity of the security regulated port in which the cleared zone is established must be informed that:

(a) access to the zone is controlled; and

(b) any unauthorised entry into the zone is an offence under these Regulations.

**6.60 Offences — unauthorised entry**

(1) A person who is required to be screened must not enter or remain in a cleared zone unless he or she has been screened and cleared.
Penalty: 50 penalty units.

(2) A person must not take a vehicle, vessel or thing into, or leave a vehicle, vessel or thing in, a cleared zone unless the vehicle, vessel or thing has been screened and cleared.

Penalty: 50 penalty units.

(3) An offence against subregulation (1) or (2) is an offence of strict liability.

Subdivision 6.2.4 Water-side restricted zones

6.65 Identification of zones

(1) The boundaries of a water-side restricted zone must be clearly identifiable.

(2) The port operator for the security regulated port in which the water-side restricted zone is established must give notice of the establishment and the boundaries of the water-side restricted zone by:
   (a) water-based identification measures (such as buoys, picket boats and booms); or
   (b) land-side signs; or
   (c) posting, publishing or broadcasting notices; or
   (d) using any other means that have the effect of informing persons in or in the vicinity of the security regulated port about the establishment of the zone and its boundaries.

6.70 Duties of port operator

(1) If the Secretary gives notice of the establishment of a water-side restricted zone, the port operator for the security regulated port in which the water-side restricted zone is established must ensure that persons who are in, or in the vicinity of, the security regulated port are informed, in accordance with the maritime security plan, that:
   (a) access to the zone is controlled; and
   (b) any unauthorised entry into the zone is an offence under these Regulations.
(2) The obligation in subregulation (1) has effect even if the zone has not yet come into force.

(3) A port operator for a security regulated port must monitor access to any water-side restricted zone established in the port.

Penalty: 200 penalty units.

(4) An offence against subregulation (3) is an offence of strict liability.

(5) A port operator must ensure that the security measures and procedures to control access to water-side restricted zones detect and deter unauthorised access to those zones.

6.75 Offences — unauthorised entry

(1) A person must not enter or remain in a water-side restricted zone unless authorised to do so by the port operator, or a port facility operator acting on behalf of the port operator, of the security regulated port in which the zone is established.

Penalty: 50 penalty units.

(2) A person must not take a vessel or thing into, or leave a vessel or thing in, a water-side restricted zone unless authorised to do so by the port operator for the security regulated port in which the zone is established.

Penalty: 50 penalty units.

(3) An offence against subregulation (1) or (2) is an offence of strict liability.

Division 6.3 Ship security zones

6.80 Exclusion zones

For subsection 107 (1) of the Act, an exclusion zone is prescribed as a type of ship security zone.
6.85 Declaration of operation of zone

(1) A port operator for a security regulated port may request the Secretary to declare that a ship security zone is to operate around a security regulated ship while the ship is in the port.

(2) A request under this regulation must be in writing and must set out:

(a) the purpose for the proposed declaration; and

(b) the boundaries of the ship security zone (that is, the distance from the security regulated ship in relation to which access is controlled); and

(c) the security measures and procedures to be taken to control access into the zone by people, vessels or things; and

(d) steps to be taken to inform people that a ship security zone has been declared and that entry into the zone without authority is an offence; and

(e) the name or position of the person or persons responsible for the security measures, procedures or steps referred to in paragraphs (c) and (d).

6.90 Identification of zones

(1) The boundaries of a ship security zone must be clearly identifiable.

(2) The port operator for the security regulated port in which the ship security zone is established must give notice of the establishment and the boundaries of the ship security zone by:

(a) water-based identification measures (such as buoys, picket boats and booms); or

(b) signs; or

(c) posting, publishing or broadcasting notices; or

(d) using any other means that have the effect of informing persons in or in the vicinity of the security regulated port about the establishment of the zone and its boundaries.
6.95 Duties of port operator

(1) If the Secretary gives notice of the establishment of a ship security zone, the port operator for the security regulated port in which the ship security zone is established must ensure that persons who are in, or in the vicinity of, the security regulated port are informed, in accordance with the maritime security plan, that:
   (a) access to the zone is controlled; and
   (b) any unauthorised entry into the zone is an offence under these Regulations.

(2) The obligation in subregulation (1) has effect even if the zone has not yet come into force.

(3) A port operator for a security regulated port must monitor access to any ship security zone established in the port.
   Penalty: 200 penalty units.

(4) An offence against subregulation (3) is an offence of strict liability.

(5) A port operator must ensure that the security measures and procedures to control access to ship security zones detect and deter unauthorised access to those zones.

6.100 Offences — unauthorised entry

(1) A person must not enter or remain in a ship security zone unless authorised to do so by the port operator for the security regulated port in which the zone operates.
   Penalty: 50 penalty units.

(2) A person must not take a vessel or thing into, or leave a vessel or thing in, a ship security zone unless authorised to do so by the port operator for the security regulated port in which the zone operates.
   Penalty: 50 penalty units.

(3) An offence against subregulation (1) or (2) is an offence of strict liability.
Division 6.4 On-board security zones

6.105 On-board restricted areas
For subsection 111(1) of the Act, an on-board restricted area is prescribed as a type of on-board security zone.

6.110 Identification of zones
The boundaries of an on-board security zone established on a regulated Australian ship must be clearly identifiable and must be permanently and sufficiently marked with signs to inform persons who are on board, or in the vicinity of, the ship that:
(a) access to the zone is controlled; and
(b) any unauthorised entry into the zone is an offence under these Regulations.

6.115 Duties of ship operators
(1) A ship operator must monitor and control access to any on-board security zones in a regulated Australian ship.
   Penalty: 200 penalty units.
(2) An offence against subregulation (1) is an offence of strict liability.
(3) A ship operator must ensure that the security measures and procedures to control access to on-board security zones detect and deter unauthorised access to those zones.

6.120 Offences — unauthorised entry
(1) A person must not enter or remain in an on-board security zone unless authorised to do so by the ship operator for the ship on which the zone is established.
   Penalty: 50 penalty units.
(2) A person must not take goods or other things into or in an on-board security zone unless authorised to do so by the ship operator for the ship on which the zone is established.
Penalty: 50 penalty units.

(3) An offence against subregulation (1) or (2) is an offence of strict liability.

Division 6.5  Offshore security zones

Subdivision 6.5.1  Preliminary

6.125  Types of offshore security zones (Act s 113B)
For subsection 113B (1) of the Act, the following are prescribed as the types of offshore security zones that the Secretary may establish:
(a) offshore facility zone;
(b) offshore water-side zone.

Subdivision 6.5.2  Offshore facility zones

6.130  Identification of zones
(1) An offshore facility zone must be clearly identifiable as an offshore security zone.

(2) Persons who are in or in the vicinity of a zone must be informed that:
(a) access to the zone is controlled; and
(b) any unauthorised entry into the zone is an offence under these Regulations.

6.135  Duties of offshore facility operator
(1) An offshore facility operator must monitor and control access to the offshore facility zone.

   Penalty: 200 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.
6.140 Offences — unauthorised entry

(1) A person must not enter or remain in an offshore facility zone unless authorised to do so by the offshore facility operator.

Penalty: 50 penalty units.

(2) An offence against subregulation (1) is an offence of strict liability.

Subdivision 6.5.3 Offshore water-side zones

6.145 Identification of zones

The operator of an offshore facility for which an offshore water-side zone is established must give notice of the establishment and the boundaries of the zone by:

(a) water based identification measures; or
(b) posting, publishing or broadcasting notices; or
(c) using any other means that have the effect of informing persons in or in the vicinity of the zone about the establishment of the zone and its boundaries.

6.150 Duties of offshore facility operator

(1) If the Secretary gives notice of the establishment of an offshore water-side zone, the offshore facility operator concerned must ensure that persons who are in, or in the vicinity of, the security regulated offshore facility are informed, in accordance with the offshore security plan, that:

(a) access to the zone is controlled; and
(b) any unauthorised entry into the zone is an offence under these Regulations.

(2) An offshore facility operator must monitor access to any offshore water-side zone.

Penalty: 200 penalty units

(3) An offence against subregulation (1) is an offence of strict liability.
(4) An offshore facility operator must ensure that the security measures and procedures to control access to offshore water-side zones detect and deter unauthorised access to those zones.

6.155 Offences – unauthorised entry

(1) A person must not enter or remain in an offshore water-side zone unless authorised to do so by the offshore facility operator concerned.

Penalty: 50 penalty units.

(2) A person must not take a vessel or thing into, or leave a vessel or thing in, an offshore water-side zone unless authorised to do so by the offshore facility operator concerned.

Penalty: 50 penalty units.

(3) An offence against subregulation (1) or (2) is an offence of strict liability.
Part 7  Other security measures

Division 7.1  Preliminary

7.05  Access not to be denied

(1) Nothing in this Part has the effect of preventing entry into a maritime security zone by a person who:
   (a) is accompanied by a law enforcement officer for the purposes of an investigation; or
   (b) is an Australian Federal Police employee, a member of the Australian Federal Police, or an officer or employee of the police force or service of a State or Territory, who requires access for the purposes of a police investigation; or
   (c) is otherwise authorised by a law of the Commonwealth, State or Territory to enter the maritime security zone.

Example for paragraph (c)
Entry to maritime security zones must not be denied to law enforcement officers, Australian Customs Service officers or AMSA officers if the entry is required in the course of their duties.

(2) Nothing in this Part has the effect of preventing a member of the Australian Defence Force who is on duty:
   (a) from entering a maritime security zone; or
   (b) from taking into a maritime security zone vessels, vehicles or goods:
      (i) for the purpose of gaining access to a ship that is under the control, or in the service, of the Australian Defence Force; or
      (ii) in connection with the movement, loading, unloading, maintenance or provisioning of such a ship.
Division 7.2 Screening and clearing

7.20 Duties of port facility operator
The port facility operator for a port facility in which a cleared zone is established must ensure that:

(a) subject to regulation 7.25, persons boarding a security regulated passenger ship:
   (i) have been screened in preparation for boarding, and cleared at the time they board the ship; or
   (ii) are screened and cleared immediately after they board the ship; and

(b) subject to regulation 7.27, baggage taken on board the ship:
   (i) has been screened in preparation for being taken on board, and cleared at the time it is taken on board the ship; or
   (ii) is screened and cleared immediately after it is taken on board the ship.

7.25 Persons who need not be screened
(1) For paragraph 115 (2) (b) of the Act, the persons mentioned in subregulation (3) may pass through a screening point without being screened when boarding a security regulated passenger ship for which maritime security level 1 is in force.

(2) For paragraph 115 (2) (c) of the Act, the persons mentioned in subregulation (3) may enter a cleared zone or board a cleared vessel other than through a screening point when maritime security level 1 is in force for the port facility in which the cleared zone is established or in which the cleared vessel is being loaded or unloaded.

(3) For subregulations (1) and (2), the persons are:
(a) in the case of a security regulated passenger ship — a member of the ship’s crew; and
(b) the CSO for the ship, while on duty; and
(c) the PFSO for the port facility in which the cleared zone is established, while on duty; and
(d) a PSO for the port in which the cleared zone is established, while on duty; and
(e) a screening officer; and
(f) a law enforcement officer; and
(g) a member of the Australian Defence Force, in the course of his or her duties; and
(h) an officer of AMSA, in the course of his or her duties; and
(i) a quarantine officer, in the course of his or her duties; and
(j) a member of a fire, ambulance, medical, search or rescue service, in the course of his or her duties; and
(k) an immigration officer, in the course of his or her duties; and
(l) a maritime security inspector, in the course of his or her duties; and
(m) a person appointed by a court to be a Marshal, when exercising a power or function, or performing a duty, conferred or imposed on him or her by the Admiralty Rules 1988; and
(n) a person authorised to exercise a power or function, or perform a duty, conferred or imposed on a Marshal under those Rules, when exercising that power or function, or performing that duty.

(4) For paragraph 115 (2) (b) of the Act, the following persons may pass through a screening point without being screened when boarding a security regulated passenger ship moored at a port facility for which maritime security level 2 or 3 is in force:
(a) a law enforcement officer; and
(b) a member of the Australian Defence Force, in the course of his or her duties; and
(c) a member of a fire, ambulance, medical, search or rescue service, in the course of his or her duties.
7.27 Goods that need not be screened

(1) For paragraph 116 (2) (b) of the Act, baggage may pass through a screening point without being screened if the baggage belongs to a person who, under subregulation 7.25 (1) or (4), need not be screened when boarding a security regulated passenger ship.

(2) For paragraph 116 (2) (c) of the Act, baggage and other goods may enter a cleared zone or be taken on board a cleared vessel other than through a screening point if the baggage and goods belong to a person who, under subregulation 7.25 (2), may enter the cleared zone or board the cleared vessel other than through the screening point.

7.28 Vehicles that need not be screened

(1) For paragraph 117 (2) (b) of the Act, a vehicle may pass through a screening point without being screened if the vehicle is being driven by a member of the Australian Defence Force who, under subregulation 7.25 (1) or (4), need not be screened when boarding a security regulated passenger ship.

(2) For paragraph 117 (2) (c) of the Act, a vehicle may enter a cleared zone or go on board a cleared vessel other than through a screening point if the vehicle is being driven by a member of the Australian Defence Force who, under subregulation 7.25 (2), may enter the cleared zone or board the cleared vessel other than through the screening point.

7.29 Vessels that need not be screened

(1) For paragraph 118 (2) (b) of the Act, a vessel may pass through a screening point without being screened if the vessel is under the control of a member of the Australian Defence Force who, under subregulation 7.25 (1) or (4), need not be screened when boarding a security regulated passenger ship.

(2) For paragraph 118 (2) (c) of the Act, a vessel may enter a cleared zone or be taken on board a cleared vessel other than through a screening point if the vessel is under the control of a member of the Australian Defence Force who, under...
subregulation 7.25 (2), may enter the cleared zone or board the cleared vessel other than through the screening point.

7.30 Equipment to be used for screening

(1) For subsection 119 (1) of the Act, the equipment to be used for screening under this Part must be capable of detecting weapons and prohibited items on persons or in baggage.

(2) The equipment may comprise a combination of screening equipment such as a walk-through metal detector, hand-held metal detector, trace explosive detection device and x-ray equipment.

7.33 Notice to be displayed at screening points

(1) For paragraph 119 (2) (l) of the Act, notices that it is an offence under the Act to carry weapons or prohibited items through a screening point must be displayed with reasonable prominence at screening points.

(2) A notice must include a list of weapons and prohibited items for the purposes of the Act.

Note 1 See section 10 of the Act and regulations 1.60 and 1.65 as to what are prohibited items and weapons.

Note 2 Sections 121 and 128 of the Act create the offences of carrying weapons and prohibited items through screening points. Certain persons are authorised, under those sections and regulation 7.45, to carry weapons or prohibited items through screening points.

7.35 Offences — screening and clearing

(1) A port facility operator must not allow a person who is required to be screened to enter a cleared zone, unless the person has been screened and cleared.

Penalty: 200 penalty units.

(2) A port facility operator must not allow goods that are required to be screened to enter a cleared zone, unless the goods have been screened and cleared.

Penalty: 200 penalty units.
(3) A port facility operator must not allow a person who is required to be screened and cleared to board a security regulated passenger ship that is moored at the facility, unless:

(a) if there is a screening point through which the person must pass at the facility — the person has been screened in preparation for boarding, and cleared at the time the person boards the ship;

(b) if there is no such screening point at the facility — the port facility operator has made arrangements with the master of the ship for the person to be screened and cleared on board the ship immediately after the person boards the ship.

Penalty: 200 penalty units.

(4) A port facility operator must not allow baggage that is required to be screened and cleared to be taken on board a security regulated passenger ship that is moored at the facility, unless:

(a) if there is a screening point through which the baggage must pass at the facility — the baggage has been screened in preparation for being taken on board the ship, and cleared at the time it is taken on board;

(b) if there is no such screening point at the facility — the port facility operator has made arrangements with the master of the ship for the baggage to be screened and cleared on board the ship immediately after the baggage is taken on board.

Penalty: 200 penalty units.

(5) A ship operator for a security regulated passenger ship must not allow a person who is required to receive clearance to board the ship, unless:

(a) the person is cleared at the time the person boards the ship; or

(b) the person is screened and cleared on board the ship immediately after the person boards the ship.

Penalty: 200 penalty units.

(6) A ship operator for a security regulated passenger ship must not allow baggage that is required to receive clearance to be taken on board the ship, unless:
(a) the baggage is cleared at the time it is taken on board the ship; or
(b) the baggage is screened and cleared on board the ship immediately after the baggage is taken on board.

Penalty: 200 penalty units.

### Division 7.3 Weapons and prohibited items

#### 7.39 Definition of licensed security guard for Division 7.3

In this Division:

*licensed security guard* means a person who holds a licence to work as a security guard, being a licence:

(a) issued or recognised by the State or Territory in which the person is working; and

(b) that is in force.

#### 7.40 Persons authorised to possess weapons or prohibited items in maritime security zones

(1) This regulation applies for sections 120 and 127 of the Act.

(2) A person is authorised to have a weapon or prohibited item in his or her possession while in a maritime security zone if the person is:

(a) a maritime security guard, an SSO, or a licensed security guard, who is on duty; or

(b) the master of a security regulated ship located in the zone who has the weapon or prohibited item in his or her possession for the purpose of securing it for carriage on board the ship; or

(c) a PSO, PFSO or screening officer, who has the weapon or prohibited item in his or her possession for the purpose of securing it for carriage on board a security regulated ship; or

(d) a veterinarian, or a quarantine officer, who has the weapon or prohibited item in his or her possession for the purpose of controlling or euthanasing animals in a maritime
security zone or on board a security regulated ship or other vessel; or

(e) a quarantine officer who has the weapon or prohibited item in his or her possession for the purpose of eradicating pests or treating diseases in a maritime security zone or on board a security regulated ship or other vessel; or

(f) an officer of a State or Territory department who has the weapon or prohibited item in his or her possession for the purpose of eradicating pests or treating diseases in a maritime security zone, or on board a security regulated ship or other vessel, under a law of the State or Territory.

(3) In addition, a person is authorised to have a weapon or prohibited item in his or her possession while in a maritime security zone if:

(a) the person is:
   (i) an inspector of the Royal Society for the Prevention of Cruelty to Animals of a State or Territory; or
   (ii) an officer of any other organisation that has as one of its objects the promotion of the welfare of, or the prevention of cruelty to, animals; and

(b) the person has the weapon or prohibited item in his or her possession in connection with carrying out an inspection related to the welfare of any animals in a maritime security zone or on board a security regulated ship; and

(c) the inspection is authorised by a law of the State or Territory in which the maritime security zone or the ship is located.

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

(1) This regulation applies for sections 121 and 128 of the Act.

(2) A person is authorised to pass through a screening point with a weapon or prohibited item in his or her possession if the person is:

(a) a maritime security guard, an SSO, or a licensed security guard, who is on duty; or
(b) the master of a security regulated ship who is passing through the screening point with the weapon or prohibited item in his or her possession for the purpose of securing it for carriage on board the ship; or

(c) a PSO, PFSO or screening officer, who is passing through the screening point with the weapon or prohibited item in his or her possession for the purpose of securing it for carriage on board a security regulated ship; or

(d) an ADF member who is on duty; or

(e) a veterinarian, or a quarantine officer, who has the weapon or prohibited item in his or her possession for the purpose of controlling or euthanasing animals in a maritime security zone or on board a security regulated ship; or

(f) a quarantine officer who has the weapon or prohibited item in his or her possession for the purpose of eradicating pests or treating diseases in a maritime security zone or on board a security regulated ship; or

(g) an officer of a State or Territory department who has the weapon or prohibited item in his or her possession for the purpose of eradicating pests or treating diseases in a maritime security zone, or on board a security regulated ship, under a law of the State or Territory.

(3) In addition, a person is authorised to pass through a screening point with a weapon or prohibited item in his or her possession if:

(a) the person is:

   (i) an inspector of the Royal Society for the Prevention of Cruelty to Animals of a State or Territory; or

   (ii) an officer of any other organisation that has as one of its objects the promotion of the welfare of, or the prevention of cruelty to, animals; and

(b) the person has the weapon or prohibited item in his or her possession in connection with carrying out an inspection related to the welfare of any animals in a maritime security zone or on board a security regulated ship; and

(c) the inspection is authorised by a law of the State or Territory in which the maritime security zone or the ship is located.
7.50 **Authorised carriage or possession of weapons or prohibited items on board regulated Australian ships**

(1) This regulation applies for sections 122, 123, 129 and 130 of the Act.

(2) A person is authorised to carry, or otherwise have in his or her possession, a weapon or prohibited item on board a regulated Australian ship if the person is:

(a) a maritime security guard, an SSO, or a licensed security guard, who is on duty; or
(b) the master of the ship, or a PSO, PFSO or screening officer, who has the weapon or prohibited item in his or her possession for the purpose of securing the weapon or prohibited item for carriage on the ship; or
(c) an ADF member who is on duty; or
(d) a veterinarian, or a quarantine officer, who has the weapon or prohibited item in his or her possession for the purpose of controlling or euthanasing animals on board the ship; or
(e) a quarantine officer who has the weapon or prohibited item in his or her possession for the purpose of eradicating pests or treating diseases on board the ship; or
(f) an officer of a State or Territory department who has the weapon or prohibited item in his or her possession for the purpose of eradicating pests or treating diseases on board the ship under a law of the State or Territory.

(3) In addition, a person is authorised to carry, or otherwise have in his or her possession, a weapon or prohibited item on board a regulated Australian ship if:

(a) the person is:

   (i) an inspector of the Royal Society for the Prevention of Cruelty to Animals of a State or Territory; or
   
   (ii) an officer of any other organisation that has as one of its objects the promotion of the welfare of, or the prevention of cruelty to, animals; and

(b) the person has the weapon or prohibited item in his or her possession in connection with carrying out an inspection related to the welfare of any animals on board the ship; and
(c) the inspection is authorised by a law of the State or Territory in which the ship is located.

7.55 **Authorisation subject to compliance with other laws**

In spite of regulations 7.40, 7.45 and 7.50, a person is not authorised to carry or possess a weapon or prohibited item in the circumstances stated in those regulations if:

(a) carriage or possession of the weapon or prohibited item is prohibited by another law of the Commonwealth, or a law of a State or Territory, without a licence, permit or authorisation; and

(b) the person does not have a licence, permit or authorisation of that kind for the weapon or prohibited item.
Part 8 Powers of officials

Division 8.1 Preliminary

Note This Division heading is reserved for future use.

Division 8.2 Maritime security inspectors

8.20A Maritime security inspectors — criteria for appointment

(1) For paragraph 136 (1) (c) of the Act, the Secretary may appoint a person to be a maritime security inspector if the Secretary is satisfied that:

(a) the person:

(i) is an IRCA certificated auditor; or

(ii) has qualifications that are equivalent to those that an IRCA certificated auditor has; or

(iii) has experience that is equivalent to the experience that an IRCA certificated auditor has; and

(b) the person:

(i) has a working knowledge of the Act and these Regulations, including the powers, functions and duties of a maritime security inspector; and

(ii) is a suitable person to access and handle security information; and

(iii) is otherwise able to perform the duties of a maritime security inspector.

(2) In this regulation:

IRCA certificated auditor means an auditor who is certified by the International Register of Certificated Auditors.
8.20 **Identity cards (Act s 137 (2))**

(1) The minimum requirements in relation to the form of an identity card for a maritime security inspector are as follows:

(a) the card must bear a recent photograph of the holder;
(b) the card must set out the holder’s name;
(c) the card must bear a statement of its date of expiry;
(d) the card must bear a statement to the effect that the holder is a maritime security inspector appointed under section 136 of the Act;
(e) the card must bear the signatures of the holder and the Secretary.

(2) If a person representing or apparently representing a maritime industry participant so requests, a maritime security inspector must show his or her identity card to the person.

Penalty: 5 penalty units.

---

**Division 8.3  Duly authorised officers**

Note This Division heading is reserved for future use.

**Division 8.4  Law enforcement officers**

8.40 **Customs officers who are law enforcement officers**

For paragraph (c) of the definition of *law enforcement officer* in section 151 of the Act, the following are prescribed:

(a) customs officers who are attached to a Customs District Office or to the Northern Territory or Tasmanian Customs Regional Offices;
(b) customs officers who are assigned customs duties associated with:
   - intelligence activities; or
   - passenger processing; or
   - compliance, investigation or enforcement of border and cargo matters.
Division 8.5  Maritime security guards

8.50  Training and qualifications
For paragraph 162 (2) (a) of the Act, the following are prescribed as training and qualification requirements for maritime security guards:
(a) the person:
   (i) must hold at least a Certificate II in Security Operations that is in force; or
   (ii) must hold a certificate or qualification that is in force and that is equivalent to at least a Certificate II in Security Operations (for example, a Certificate II in Security (Guarding)); or
   (iii) must have undergone training and acquired experience while working as a security guard that is sufficient to satisfy the requirements for obtaining a security guard license in the state or territory where the person intends to work as a maritime security guard (the relevant state or territory);
(b) the person must hold a licence to work as a security guard, being a licence that was issued or recognised by the relevant state or territory and that is in force;
(c) the person must have a working knowledge of the Act and these Regulations, including knowledge about how to restrain and detain persons in accordance with section 163 of the Act.

8.55  Identity cards (Act s 162 (2) (b))
(1) The requirements in relation to the issue and use of an identity card for a maritime security guard are as follows:
(a) the card must be issued by the employer of the maritime security guard;
(b) the card must be displayed by the maritime security guard while he or she is on duty.
(2) The minimum requirements in relation to the form of the identity card are as follows:
   (a) the card must bear a recent photograph of the maritime security guard;
   (b) the card must set out the guard’s name;
   (c) the card must bear a statement of its date of expiry;
   (d) the card must bear the name of the employer that issued the card.

Division 8.6 Screening officers

8.60 Training and qualifications

For paragraph 165 (2) (a) of the Act, the following are prescribed as training and qualification requirements for screening officers:

(a) the person:
   (i) must hold at least a Certificate II in Security Operations that is in force; or
   (ii) must hold a certificate or qualification that is in force and that is equivalent to at least a Certificate II in Security Operations (for example, a Certificate II in Security (Guarding)); or
   (iii) must have undergone training and acquired experience while working as a security guard that is sufficient to satisfy the requirements for obtaining a security guard license in the state or territory where the person intends to work as a screening officer (the relevant state or territory);

(b) the person must hold a licence to work as a security guard, being a licence that was issued or recognised by the relevant state or territory and that is in force;

(c) the person must be competent in:
   (i) maintaining the integrity of a cleared zone; and
   (ii) using screening equipment; and
   (iii) the methods and techniques to be used for screening persons, baggage and other goods; and
(iv) dealing with weapons and prohibited items that are detected or surrendered;
(d) the person must have a working knowledge of the Act and these Regulations, including knowledge about how to restrain and detain persons in accordance with section 167 of the Act.

8.65 **Identity cards (Act s 165 (2) (b))**

(1) The requirements in relation to the issue and use of an identity card for a screening officer are as follows:
   (a) the card must be issued by the person who authorised or required the officer to conduct screening;
   (b) the card must be displayed by the screening officer while he or she is on duty.

(2) The minimum requirements in relation to the form of the identity card are as follows:
   (a) the card must bear a recent photograph of the screening officer;
   (b) the card must set out the officer’s name;
   (c) the card must bear a statement of its date of expiry;
   (d) the card must bear the name of the person who issued the card.
Part 9  
**Reporting maritime transport or offshore facility security incidents**

*Note*  This Part heading is reserved for future use.

Part 10  
**Information-gathering**

*Note*  This Part heading is reserved for future use.
Part 11 Enforcement

Division 11.2 Infringement notices

11.05 Purpose and effect of Division

(1) The purpose of this Division is to create a system of infringement notices for certain offences against the Act and these Regulations as an alternative to prosecution.

(2) This Division does not:
   (a) require an infringement notice to be issued to a person for an offence; or
   (b) affect the liability of a person to be prosecuted for an offence if an infringement notice is not issued to the person for the offence; or
   (c) prevent the issue of 2 or more infringement notices to a person for an offence; or
   (d) affect the liability of a person to be prosecuted for an offence if the person does not comply with an infringement notice for the offence; or
   (e) limit or otherwise affect the penalty that may be imposed by a court on a person convicted of an offence.

11.10 Definition for Division — authorised person

In this Division:

authorised person means:
   (a) a law enforcement officer; or
   (b) a maritime security inspector.

11.15 Amount of penalty if infringement notice issued

The penalty for an offence payable under an infringement notice issued to a person for the offence is one-fifth of the maximum penalty that a court could impose on the person for the offence.
11.20 Authorised persons may issue infringement notices

(1) In this regulation:

infringement notice offence means an offence:

(a) against any provision of the Act (other than subsection 43 (1), 62 (1) or 100C (1)) a contravention of which is an offence of strict liability; or

(b) against a provision of these Regulations (being an offence that is an offence of strict liability).

(2) If an authorised person has reason to believe that a person has committed an infringement notice offence, the authorised person may issue a notice (called an infringement notice) to the person for the offence.

11.25 Contents of infringement notice

(1) An infringement notice:

(a) must bear a unique number; and

(b) must state the name of the authorised person who issued it, and:

(i) if he or she is a law enforcement officer (other than a customs officer) — the name of the police force or police service of which he or she is a member; or

(ii) if he or she is a customs officer or a maritime security inspector — that fact; and

(c) must state its date of issue; and

(d) must state the full name, or the surname and initials, and the address, of the person to whom it is issued; and

(e) must give brief details of the alleged offence for which it is issued, including:

(i) the date and time of the offence; and

(ii) where the offence happened; and

(iii) the provision of the Act or these Regulations contravened; and

(f) must state the penalty for the offence payable under the notice; and
(g) must state where and how that penalty can be paid (including, if the penalty can be paid by posting the payment, the place to which it should be posted); and

(h) must state that if the person to whom it is issued (the recipient) pays the penalty within 28 days after the day when the notice is served (or any longer time allowed in writing by the Secretary), then:

(i) any liability of the recipient for the offence will be discharged; and

(ii) the recipient will not be prosecuted in a court for the offence; and

(iii) the recipient will not be taken to have been convicted of the offence; and

(i) must state the greatest penalty that a court could impose on the recipient for the offence; and

(j) must state the number of demerit points that the recipient will accrue for the offence; and

(k) must state that if the recipient is prosecuted in court and found guilty of the offence:

(i) the recipient may be convicted of the offence and ordered to pay a penalty and costs; and

(ii) will be subject to any other order that the court makes; and

(iii) will accrue the number of demerit points specified in the notice; and

(l) must state how and to whom the recipient can apply to be allowed more time to pay the penalty; and

(m) must be signed by the authorised person who issued it.

(2) An infringement notice may contain any other information that the authorised person who issues it thinks necessary.

11.30 **Service of infringement notices**

(1) An infringement notice must be served on the person to whom it is issued.

(2) An infringement notice may be served on an individual:

(a) by giving it to the individual; or
(b) by leaving it at, or by sending it by post, telex, fax or similar facility to, the address of the place of residence or business (the relevant place) of the individual last known to the authorised person who issues it; or

(c) by giving it, at the relevant place, to someone who:
   (i) lives or is employed, or apparently lives or is employed, there; and
   (ii) is, or the authorised person who issues it has reason to believe is, over 16 years of age.

(3) An infringement notice may be served on a corporation:
   (a) by leaving it at, or by sending it by post, telex, fax or similar facility to, the address of the head office, a registered office or a principal office of the corporation; or
   (b) by giving it, at an office mentioned in paragraph (a), to someone who is, or the authorised person who issues it has reason to believe is, an officer or employee of the corporation.

11.35 Time for payment of penalty
The penalty stated in an infringement notice must be paid:
   (a) within 28 days after the day on which the notice is served on the person to whom it is issued; or
   (b) if the person applies for a further period of time in which to pay the penalty, and that application is granted — within the further period allowed; or
   (c) if the person applies for a further period of time in which to pay the penalty, and the application is refused — within 7 days after the notice of the refusal is served on the person; or
   (d) if the person applies for the notice to be withdrawn, and the application is refused — within 28 days after the notice of the refusal is served on the person.

11.40 Extension of time to pay penalty
   (1) The person to whom an infringement notice is issued (the recipient) may apply, in writing, to the Secretary for a further
period of up to 28 days in which to pay the penalty stated in the notice.

(2) Within 14 days after receiving the application, the Secretary:
   (a) must grant or refuse a further period not longer than the period sought; and
   (b) must notify the recipient in writing of the decision and, if the decision is a refusal, the reasons for it.

(3) Notice of the decision may be served on the recipient in any way in which the infringement notice could have been served on the recipient.

11.45 Payment of penalty

(1) An infringement notice penalty is not paid until the whole of the amount of the penalty has been received by the Commonwealth.

(2) In particular, if the Commonwealth accepts a cheque in payment of a penalty or part of a penalty, the penalty is not paid until the cheque has been honoured.

11.50 Effect of payment of penalty

(1) If the person to whom an infringement notice is issued for an offence pays the penalty stated in the notice:
   (a) any liability of the person for the offence is discharged; and
   (b) the person may not be prosecuted in a court for the offence; and
   (c) the person is not taken to have been convicted of the offence.

(2) If 2 or more infringement notices are issued to a person for the same offence, the person’s liability to be prosecuted for the offence ceases if the person pays the penalty stated in any of the notices.
11.55 Withdrawal of infringement notice

(1) Before the end of 28 days after receiving an infringement notice, a person may apply, in writing, to the Secretary for the infringement notice to be withdrawn.

(2) The application must set out the facts or matters that the person believes the Secretary should take into account in relation to the offence alleged in the infringement notice.

(3) Within 14 days after receiving the application, the Secretary must:
   (a) withdraw or refuse to withdraw the notice; and
   (b) notify the person in writing of the decision and, if the decision is a refusal, the reasons for the decision.

(4) If the Secretary has not approved, or refused to approve, the withdrawal of the notice within the period allowed by subregulation (3), the Secretary is taken to have refused to approve the withdrawal of the notice.

(5) Before withdrawing or refusing to withdraw a notice, the Secretary must consider:
   (a) whether the person has been convicted previously of an offence against the Act or these Regulations; and
   (b) the circumstances of the offence stated in the notice; and
   (c) whether the person has previously paid a penalty under an infringement notice issued to the person for an offence of the same type as the offence mentioned in the notice; and
   (d) any other relevant matter.

(6) The Secretary may also withdraw an infringement notice on his or her own initiative.

11.60 Notice of withdrawal of infringement notices

(1) Notice of the withdrawal of an infringement notice may be served on a person in any way in which the infringement notice could have been served on the person.
(2) A notice withdrawing an infringement notice:
(a) must include the following information:
   (i) the full name, or surname and initials, and address of
       the person on whom the infringement notice was
       served;
   (ii) the number of the infringement notice;
   (iii) the date of issue of the infringement notice; and
(b) must state that the notice is withdrawn; and
(c) if the Secretary intends to prosecute the person in a court
   for the relevant offence, must state that the person may be
   prosecuted in a court for the offence.

11.65 Refund of penalty etc if infringement notice
       withdrawn

(1) If an infringement notice is withdrawn after the penalty stated
    in it has been paid:
   (a) the Commonwealth must refund the amount of the penalty
       to the person who paid it; and
   (b) any demerit points accrued because of the payment are
       cancelled.

(2) If the cancelled demerit points had been accumulated in respect
    of a ship, the number of demerit points accumulated in respect
    of the ship decreases by that number of demerit points.

11.70 Evidence of certain matters in relation to
       infringement notices

(1) At the hearing of a prosecution for an offence in relation to
    which an infringement notice has been issued, a certificate of
    any of the following kinds, signed on behalf of the Secretary, is
    evidence of the facts stated in it:
   (a) a certificate stating that:
      (i) the infringement notice was served on the alleged
          offender; and
      (ii) the infringement notice penalty has not been paid in
          accordance with this Division;
11.75 Effect of certain admissions

Evidence of an admission made by a person in an application under regulation 11.55 is not admissible in proceedings against the person for the relevant alleged offence unless the person introduces the application into evidence.

11.80 Matter not to be taken into account in determining sentence

If a person to whom an infringement notice has been issued:
(a) does not pay the infringement notice penalty; and
(b) is prosecuted for, and convicted of, the alleged offence mentioned in the infringement notice;
the court must not, in determining the penalty to be imposed, take into account the fact that the person did not pay the infringement notice penalty.
**Division 11.6  Demerit points system**

**11.300  Purpose of Division**

This Division establishes a demerit points system under which the approval of a maritime security plan, a ship security plan or an offshore security plan may be cancelled.

**11.305  Accrual of demerit points by maritime industry participants**

(1) If a maritime industry participant:

(a) is issued with an infringement notice, and pays the infringement notice penalty; or

(b) is convicted or found guilty of an offence;

the participant accrues 1 demerit point for each penalty unit of:

(c) the maximum number of penalty units that a court could impose on the participant for the alleged offence; or

(d) if the penalty for the offence is a term of imprisonment — the maximum number of penalty units that the court could impose in lieu of imprisonment.

(2) To avoid doubt, a reference in subregulation (1) to the maximum number of penalty units that a court could impose is, if the alleged offender is a corporation, the maximum number that the court could impose taking into account subsection 4B (3) of the *Crimes Act 1914*.

**11.310  Accumulation of demerit points in respect of ships**

Demerit points are accumulated in respect of a ship only if a ship operator accrues the demerit points because the operator:

(a) has been convicted or found guilty of an offence against section 62 or 63 of the Act in respect of the ship; or

(b) has been issued with an infringement notice for an offence against section 63 of the Act in respect of the ship, and has paid the infringement notice penalty as an alternative to prosecution.
11.315 Expiry of demerit points
A demerit point expires 5 years after it is accrued.

11.320 Demerit points — maritime security plans
For section 199 of the Act, the approval of the maritime security plan of a maritime industry participant may be cancelled if the participant accrues:
(a) in the case of a maritime industry participant who is an individual — 600 demerit points; or
(b) in any other case — 3 000 demerit points.

11.325 Demerit points — ship security plans
For section 200 of the Act, the approval of a ship security plan may be cancelled if 3 000 demerit points are accumulated in respect of the ship.

11.330 Demerit points — offshore security plans
For section 200A of the Act, the approval of the offshore security plan of an offshore industry participant may be cancelled if the participant accrues:
(a) in the case of an offshore industry participant who is an individual — 600 demerit points; or
(b) in any other case — 3 000 demerit points.

11.335 Register of demerit points
(1) The Secretary must keep a register of demerit points accrued.
(2) The register may be kept by means of, or partly by means of, a computer system.
(3) The register must record, for each maritime industry participant:
   (a) for each offence against the Act or these Regulations of which the participant has been convicted or found guilty:
      (i) the number of demerit points accrued for the offence; and
(ii) the basis on which the number of demerit points was calculated; and

(iii) the dates on which those demerit points were accrued, and will expire; and

(iv) whether the demerit points were accumulated in respect of a ship and if so what ship; and

(b) for each alleged offence against the Act or these Regulations for which an infringement notice has been issued to the participant, and for which the participant has paid the infringement notice penalty:

(i) the number of demerit points accrued for the alleged offence; and

(ii) the basis on which the number of demerit points was calculated; and

(iii) the dates on which those demerit points were accrued, and will expire; and

(iv) whether the demerit points were accumulated in respect of a ship and if so what ship; and

(c) the total number of demerit points, other than demerit points that have expired, that the participant has accrued.

(4) The register must also record, for each ship in respect of which demerit points have been accumulated:

(a) a reference to the record in the register of each relevant accrual of demerit points by a maritime industry participant; and

(b) the total number of demerit points, other than demerit points that have expired, accumulated in respect of the ship.

(5) The Secretary must allow a maritime industry participant, at a reasonable time and on reasonable notice, to inspect the record of the participant’s accrued demerit points.

(6) The Secretary must allow a ship operator, at a reasonable time and on reasonable notice, to inspect the record of demerit points accumulated in respect of a ship operated by the operator.
Part 12  Review of decisions

Note  This Part heading is reserved for future use.
Part 13  Miscellaneous

13.05  Ship security alert systems

(1) A regulated Australian ship must be provided with a ship security alert system:
   (a) for a ship constructed on or after 1 July 2004 — before registration of the ship under the *Shipping Registration Act 1981*; and
   (b) for a passenger ship (including a high-speed passenger craft) constructed before 1 July 2004 — not later than the first survey of the ship’s radio installation after 1 July 2004; and
   (c) for an oil tanker, chemical tanker, gas carrier, bulk carrier or a cargo high speed craft, 500 gross tonnage or more, constructed before 1 July 2004 — not later than the first survey of the ship’s radio installation after 1 July 2004; and
   (d) for any other cargo ship 500 gross tonnage or more or mobile offshore drilling unit constructed before 1 July 2004 — not later than the first survey of the ship’s radio installation after 1 July 2006.

(2) A ship security alert:
   (a) must be capable of transmitting a ship-to-shore security alert identifying the ship, giving its location and indicating that the security of the ship is, or was, under threat; and
   (b) must otherwise comply with regulation XI-2/6 of the SOLAS Convention.
Notes to the *Maritime Transport and Offshore Facilities Security Regulations 2003*

**Note 1**


Under the *Legislative Instruments Act 2003*, which came into force on 1 January 2005, it is a requirement for all non-exempt legislative instruments to be registered on the Federal Register of Legislative Instruments. From 1 January 2005 the Statutory Rules series ceased to exist and was replaced with Select Legislative Instruments (SLI series). Numbering conventions remain the same, ie Year and Number.

### Table of Instruments

<table>
<thead>
<tr>
<th>Year and number</th>
<th>Date of notification in Gazette and FRLI registration</th>
<th>Date of commencement</th>
<th>Application, saving or transitional provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003 No. 366</td>
<td>23 Dec 2003</td>
<td>Part 1, Part 3 (except Subdivision 3.4.1), Part 4, rr. 6.05, 6.20, 6.80, 6.85, 6.105, Part 12 and Part 13: 1 Jan 2004 Remainder: [see r. 2]</td>
<td></td>
</tr>
<tr>
<td>2004 No. 34</td>
<td>18 Mar 2004</td>
<td>Rr. 1–3 and Schedule 1: 18 Mar 2004 Remainder: 1 July 2004 (see r. 2 (b) and Gazette 2004, No. GN11)</td>
<td></td>
</tr>
<tr>
<td>2004 No. 137</td>
<td>18 June 2004</td>
<td>Rr. 1–4 and Schedule 1: 18 June 2004 Remainder: 1 July 2004 (see r. 2 (b) and Gazette 2004, No. GN11)</td>
<td></td>
</tr>
<tr>
<td>2004 No. 195</td>
<td>1 July 2004</td>
<td>Rr. 1–4 and Schedule 1: 1 July 2004 Remainder: 1 July 2004 (see r. 2 (b) and Gazette 2004, No. GN11)</td>
<td></td>
</tr>
<tr>
<td>2005 No. 115</td>
<td>8 June 2005 (see F2005L01407)</td>
<td>9 June 2005</td>
<td>—</td>
</tr>
</tbody>
</table>

176 *Maritime Transport and Offshore Facilities Security Regulations 2003*
| Year and number | Date of notification in Gazette and FRLI registration | Date of commencement | Application, saving or transitional provisions |
|(120,504),(659,515) | 8 July 2005 (see F2005L01919) | 9 July 2005 | — |
| 2005 No. 201 | 2 Sept 2005 (see F2005L02436) | 9 July 2005 | — |
| 2005 No. 225 | 7 Oct 2005 (see F2005L03031) | 8 Oct 2005 | — |
| 2006 No. 186 | 14 July 2006 (see F2006L02347) | 15 July 2006 | — |
## Table of Amendments

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Part 1</strong></td>
<td></td>
</tr>
<tr>
<td>R. 1.01</td>
<td>am. 2005 No. 158</td>
</tr>
<tr>
<td>R. 1.02</td>
<td>am. 2005 No. 209</td>
</tr>
<tr>
<td>R. 1.03</td>
<td>am. 2004 Nos. 34 and 137; 2005 Nos. 158 and 201</td>
</tr>
<tr>
<td>R. 1.04</td>
<td>am. 2005 No. 158</td>
</tr>
<tr>
<td>R. 1.05</td>
<td>rs. 2004 No. 34</td>
</tr>
<tr>
<td>R. 1.06</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 1.32</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 1.33</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 1.34</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 1.35</td>
<td>am. 2005 No. 158</td>
</tr>
<tr>
<td>R. 1.45</td>
<td>am. 2005 Nos. 158 and 201</td>
</tr>
<tr>
<td>R. 1.50</td>
<td>am. 2005 No. 158</td>
</tr>
<tr>
<td>Heading to r. 1.55</td>
<td>rs. 2004 No. 34</td>
</tr>
<tr>
<td>R. 1.55</td>
<td>am. 2004 Nos. 34 and 137; 2005 No. 158</td>
</tr>
<tr>
<td>R. 1.56</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td></td>
<td>am. 2005 No. 158</td>
</tr>
<tr>
<td>R. 1.65</td>
<td>am. 2005 No. 158</td>
</tr>
<tr>
<td>R. 1.75</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>R. 1.80</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td><strong>Part 2</strong></td>
<td></td>
</tr>
<tr>
<td>Div. 2.2</td>
<td></td>
</tr>
<tr>
<td>Div. 2.2 of Part 2</td>
<td>rs. 2004 No. 34</td>
</tr>
<tr>
<td>Note to Div. 2.2</td>
<td>rep. 2004 No. 34</td>
</tr>
<tr>
<td>R. 2.25</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td><strong>Division 2.3</strong></td>
<td></td>
</tr>
<tr>
<td>R. 2.30</td>
<td>am. 2005 Nos. 158 and 201</td>
</tr>
<tr>
<td>R. 2.35</td>
<td>rs. 2004 No. 34</td>
</tr>
<tr>
<td></td>
<td>am. 2005 Nos. 158 and 201</td>
</tr>
<tr>
<td><strong>Part 3</strong></td>
<td></td>
</tr>
<tr>
<td>Division 3.1</td>
<td></td>
</tr>
<tr>
<td>R. 3.12</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td><strong>Division 3.2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subdivision 3.2.1</strong></td>
<td></td>
</tr>
<tr>
<td>R. 3.35</td>
<td>am. 2004 No. 34</td>
</tr>
<tr>
<td>R. 3.77</td>
<td>ad. 2004 No. 137</td>
</tr>
</tbody>
</table>
### Table of Amendments

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Division 3.3</strong></td>
<td></td>
</tr>
<tr>
<td>Subdivision 3.3.1</td>
<td></td>
</tr>
<tr>
<td>R. 3.106</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>R. 3.160</td>
<td>am. 2004 No. 137</td>
</tr>
<tr>
<td><strong>Division 3.4</strong></td>
<td></td>
</tr>
<tr>
<td>Subdivision 3.4.2</td>
<td></td>
</tr>
<tr>
<td>R. 3.191</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>R. 3.210</td>
<td>am. 2004 No. 34</td>
</tr>
<tr>
<td><strong>Part 4</strong></td>
<td></td>
</tr>
<tr>
<td>Division 4.2</td>
<td></td>
</tr>
<tr>
<td>R. 4.20</td>
<td>am. 2004 No. 34</td>
</tr>
<tr>
<td>R. 4.31</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>R. 4.45</td>
<td>am. 2004 No. 34; 2005 No. 158</td>
</tr>
<tr>
<td>R. 4.65</td>
<td>am. 2004 No. 137</td>
</tr>
<tr>
<td>R. 4.80</td>
<td>am. 2004 Nos. 34 and 195</td>
</tr>
<tr>
<td>R. 4.85</td>
<td>rs. 2005 Nos. 158 and 201</td>
</tr>
<tr>
<td>R. 4.100</td>
<td>am. 2004 No. 34</td>
</tr>
<tr>
<td><strong>Division 4.4</strong></td>
<td></td>
</tr>
<tr>
<td>Div. 4.4 of Part 4</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>Note to Div. 4.4 of Part 4</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td><strong>Division 4.5</strong></td>
<td></td>
</tr>
<tr>
<td>Div. 4.5 of Part 4</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>R. 4.140</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>R. 4.145</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td><strong>Part 5</strong></td>
<td></td>
</tr>
<tr>
<td>Division 5.1</td>
<td>rs. 2004 No. 34</td>
</tr>
<tr>
<td>Note to Div. 5.1 of Part 5</td>
<td>rep. 2004 No. 34</td>
</tr>
<tr>
<td>R. 5.10</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td></td>
<td>am. 2004 No. 195</td>
</tr>
<tr>
<td><strong>Division 5.2</strong></td>
<td>rs. 2004 No. 34</td>
</tr>
<tr>
<td><strong>Part 5A</strong></td>
<td></td>
</tr>
<tr>
<td>R. 5A.05</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td><strong>Division 5A.1</strong></td>
<td></td>
</tr>
<tr>
<td>R. 5A.05</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.10</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td></td>
<td>am. 2005 No. 201</td>
</tr>
<tr>
<td>R. 5A.12</td>
<td>ad. 2005 No. 201</td>
</tr>
</tbody>
</table>
Table of Amendments

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>R. 5A.15</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td></td>
<td>rep. 2005 No. 201</td>
</tr>
<tr>
<td></td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 5A.20</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td><strong>Division 5A.2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subdivision 5A.2.1</strong></td>
<td></td>
</tr>
<tr>
<td>R. 5A.25</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.30</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.35</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.40</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.45</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.50</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.55</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.60</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.65</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.70</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.75</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.80</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.85</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>Note to r. 5A.85</td>
<td>rep. 2005 No. 201</td>
</tr>
<tr>
<td>R. 5A.90</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td><strong>Subdivision 5A.2.2</strong></td>
<td></td>
</tr>
<tr>
<td>R. 5A.95</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.100</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.105</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td><strong>Division 5A.3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subdivision 5A.3.1</strong></td>
<td></td>
</tr>
<tr>
<td>R. 5A.110</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td><strong>Subdivision 5A.3.2</strong></td>
<td></td>
</tr>
<tr>
<td>R. 5A.115</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.120</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.125</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.130</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.135</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.140</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.145</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.150</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.155</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.160</td>
<td>ad. 2005 No. 158</td>
</tr>
</tbody>
</table>
### Table of Amendments

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>R. 5A.165</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.170</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td>R. 5A.175</td>
<td>ad. 2005 No. 158</td>
</tr>
</tbody>
</table>

**Part 6**

**Division 6.1**

- Heading to r. 6.05       | rs. 2004 No. 137 |
- R. 6.05                  | am. 2004 No. 137 |

**Division 6.1A**

- Div. 6.1A of Part 6      | ad. 2005 No. 201 |

**Subdivision 6.1A.1**

- R. 6.07A                 | ad. 2005 No. 201 |
- R. 6.07B                 | ad. 2005 No. 201 |
- R. 6.07C                 | ad. 2005 No. 201 |
- R. 6.07D                 | ad. 2005 No. 201 |
- R. 6.07E                 | ad. 2005 No. 201 |
- R. 6.07F                 | ad. 2005 No. 201 |
- R. 6.07G                 | ad. 2005 No. 201 |
- R. 6.07H                 | ad. 2005 No. 201 |

**Subdivision 6.1A.1A**

- Subdiv. 6.1A.1A          | ad. 2006 No. 202 |

**Subdivision 6.1A.2**

- R. 6.07I                 | ad. 2005 No. 201 |
- R. 6.07J                 | ad. 2005 No. 201 |
- R. 6.07K                 | ad. 2005 No. 201 |
- R. 6.07L                 | ad. 2005 No. 201 |
- R. 6.07M                 | ad. 2005 No. 201 |
- R. 6.07N                 | ad. 2005 No. 201 |

**Subdivision 6.1A.3**

- Heading to Subdiv. 6.1A.3 | rep. 2006 No. 202 |
- Heading to Subdiv. 6.1A.3 | ad. 2006 No. 202 |
- R. 6.07O                 | ad. 2005 No. 201 |
- R. 6.07P                 | ad. 2005 No. 201 |
### Table of Amendments

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>R. 6.07Q</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.07R</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.07S</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.07T</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.07U</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.07V</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.07W</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.07X</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.07Y</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.07Z</td>
<td>ad. 2005 No. 201</td>
</tr>
</tbody>
</table>

**Subdivision 6.1A.4**

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>R. 6.08A</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08B</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08C</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08D</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08E</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08F</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08G</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08H</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08I</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08J</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08K</td>
<td>am. 2006 No. 186</td>
</tr>
<tr>
<td>R. 6.08L</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08M</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08N</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08O</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08P</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08Q</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08R</td>
<td>ad. 2005 No. 201</td>
</tr>
</tbody>
</table>

**Subdivision 6.1A.5**

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>R. 6.08S</td>
<td>ad. 2005 No. 201</td>
</tr>
</tbody>
</table>

**Subdivision 6.1A.6**

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>R. 6.08T</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08U</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08V</td>
<td>ad. 2005 No. 201</td>
</tr>
</tbody>
</table>

**Subdivision 6.1A.7**

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>R. 6.08W</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08X</td>
<td>ad. 2005 No. 201</td>
</tr>
</tbody>
</table>
Table of Amendments

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>R. 6.08Y..............</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.08Z..............</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td><strong>Subdivision 6.1A.8</strong></td>
<td></td>
</tr>
<tr>
<td>R. 6.09A..............</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td><strong>Division 6.2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subdivision 6.2.2</strong></td>
<td></td>
</tr>
<tr>
<td>R. 6.33................</td>
<td>ad. 2004 No. 137</td>
</tr>
<tr>
<td>R. 6.40................</td>
<td>am. 2004 No. 137</td>
</tr>
<tr>
<td>R. 6.45................</td>
<td>am. 2004 No. 137</td>
</tr>
<tr>
<td><strong>Subdivision 6.2.4</strong></td>
<td></td>
</tr>
<tr>
<td>R. 6.65................</td>
<td>rs. 2004 No. 34</td>
</tr>
<tr>
<td></td>
<td>am. 2004 No. 137</td>
</tr>
<tr>
<td>R. 6.70................</td>
<td>rs. 2005 No. 115</td>
</tr>
<tr>
<td><strong>Division 6.3</strong></td>
<td></td>
</tr>
<tr>
<td>R. 6.90................</td>
<td>am. 2005 No. 115</td>
</tr>
<tr>
<td>R. 6.95................</td>
<td>rs. 2005 No. 115</td>
</tr>
<tr>
<td><strong>Division 6.5</strong></td>
<td></td>
</tr>
<tr>
<td>Div. 6.5 of Part 6.....</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td></td>
<td>rep. 2005 No. 201</td>
</tr>
<tr>
<td></td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td><strong>Subdivision 6.5.1</strong></td>
<td></td>
</tr>
<tr>
<td>Heading to Subdiv. 6.5.1</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.125................</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td></td>
<td>rep. 2005 No. 201</td>
</tr>
<tr>
<td></td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td><strong>Subdivision 6.5.2</strong></td>
<td></td>
</tr>
<tr>
<td>Heading to Subdiv. 6.5.2</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.130................</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td></td>
<td>rep. 2005 No. 201</td>
</tr>
<tr>
<td></td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.135................</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td></td>
<td>rep. 2005 No. 201</td>
</tr>
<tr>
<td></td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.140................</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td></td>
<td>rep. 2005 No. 201</td>
</tr>
<tr>
<td></td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td><strong>Subdivision 6.5.3</strong></td>
<td></td>
</tr>
<tr>
<td>Heading to Subdiv. 6.5.3</td>
<td>ad. 2005 No. 201</td>
</tr>
<tr>
<td>R. 6.145................</td>
<td>ad. 2005 No. 158</td>
</tr>
<tr>
<td></td>
<td>rep. 2005 No. 201</td>
</tr>
<tr>
<td></td>
<td>ad. 2005 No. 201</td>
</tr>
</tbody>
</table>
### Table of Amendments

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>R. 7.05</td>
<td>rs. 2004 No. 137</td>
</tr>
<tr>
<td>R. 7.20</td>
<td>am. 2004 No. 137</td>
</tr>
<tr>
<td>R. 7.25</td>
<td>am. 2004 No. 137; 2005 No. 115</td>
</tr>
<tr>
<td>R. 7.27</td>
<td>ad. 2004 No. 137</td>
</tr>
<tr>
<td>R. 7.28</td>
<td>ad. 2004 No. 137</td>
</tr>
<tr>
<td>R. 7.29</td>
<td>ad. 2004 No. 137</td>
</tr>
<tr>
<td>R. 7.33</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>R. 7.35</td>
<td>am. 2004 No. 137</td>
</tr>
<tr>
<td>Div. 7.3 of Part 7</td>
<td>rs. 2005 No. 115</td>
</tr>
<tr>
<td>R. 7.39</td>
<td>ad. 2005 No. 115</td>
</tr>
<tr>
<td>Heading to r. 7.40</td>
<td>rs. 2004 No. 137; 2005 No. 115</td>
</tr>
<tr>
<td>R. 7.40</td>
<td>am. 2004 Nos. 34 and 137 rs. 2005 No. 115</td>
</tr>
<tr>
<td>R. 7.45</td>
<td>rs. 2005 No. 115</td>
</tr>
<tr>
<td>R. 7.50</td>
<td>am. 2004 No. 34 rs. 2005 No. 115</td>
</tr>
<tr>
<td>R. 7.55</td>
<td>ad. 2005 No. 115</td>
</tr>
<tr>
<td>Div. 8.2 of Part 8</td>
<td>rs. 2004 No. 34</td>
</tr>
<tr>
<td>Note to Div. 8.2 of Part 8</td>
<td>rep. 2004 No. 34</td>
</tr>
<tr>
<td>R. 8.20A</td>
<td>ad. 2005 No. 115</td>
</tr>
<tr>
<td>R. 8.20</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>Div. 8.5 of Part 8</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>R. 8.50</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>R. 8.55</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>Div. 8.6 of Part 8</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>R. 8.60</td>
<td>ad. 2004 No. 34</td>
</tr>
</tbody>
</table>
### Table of Amendments

<table>
<thead>
<tr>
<th>Provision affected</th>
<th>How affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>R. 8.65</td>
<td>ad. 2004 No. 34</td>
</tr>
<tr>
<td>Part 9</td>
<td></td>
</tr>
<tr>
<td>Part 9</td>
<td>rs. 2005 Nos. 158 and 201</td>
</tr>
<tr>
<td>Part 11</td>
<td></td>
</tr>
<tr>
<td>Part 11</td>
<td>rs. 2005 No. 225</td>
</tr>
<tr>
<td>Note to Part 11</td>
<td>rep. 2005 No. 225</td>
</tr>
<tr>
<td>Div. 11.2</td>
<td></td>
</tr>
<tr>
<td>Div. 11.2 of Part 11</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.05</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.10</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.15</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.20</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.25</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.30</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.35</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.40</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.45</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.50</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.55</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.60</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.65</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.70</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.75</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.80</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>Division 11.6</td>
<td></td>
</tr>
<tr>
<td>Div. 11.6 of Part 11</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.300</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.305</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.310</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.315</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.320</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.325</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.330</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>R. 11.335</td>
<td>ad. 2005 No. 225</td>
</tr>
<tr>
<td>Part 13</td>
<td></td>
</tr>
<tr>
<td>R. 13.05</td>
<td>am. 2004 No. 34</td>
</tr>
</tbody>
</table>