Queensland

Transport Security (Counter-Terrorism) Act 2008

Current as at 25 August 2017

Queensland

Transport Security (Counter-Terrorism) Act 2008

Contents

Transport Security (Counter-Terrorism) Act 2008

An Act to make particular provision for reducing risks arising out of terrorist acts against particular surface transport operations

Chapter 1 Preliminary

Part 1 General

1 Short title

This Act may be cited as the *Transport Security (Counter-Terrorism) Act 2008*.

2 Commencement

This Act commences on a day to be fixed by proclamation.

3 Main purpose

(1) The main purpose of this Act is to provide for planning for the protection of particular surface transport operations and their users against significant adverse impacts associated with terrorist acts involving those surface transport operations.

(2) This Act achieves the main purpose by—

(a) providing for the declaration of particular surface transport operations as security-identified surface transport operations; and

(b) establishing a regulatory framework for the preparation, implementation and review of risk management plans—

(i) addressing and mitigating the risks of terrorist acts for those surface transport operations; and

(ii) providing for the recovery and continuity of those surface transport operations in the event of a terrorist act.

4 Overall objectives

The overall objectives of this Act are the following—

(a) to achieve an appropriate balance in relation to the security of SISTOs, public confidence, and the cost of requirements under this Act on SISTOs;

(b) to promote efficient and affordable counter-terrorism measures for SISTOs and an overall benefit for the community in the security-preparedness of SISTOs;

(c) to take into account relevant national and international benchmarks for best practice;

(d) to promote consultation, communication and cooperation between the government, surface transport operations and the community;

(e) to seek voluntary compliance in preference to enforcement.

5 Act binds all persons

(1) This Act binds all persons, including the State, and so far as the legislative power of the Parliament permits, the other States and the Commonwealth.

(2) Nothing in this Act makes a State or the Commonwealth liable to be prosecuted for an offence.

6 Relationship to other Acts

This Act is in addition to, and does not limit any other Act that makes provision for the safety of the public, including, for example, the following Acts—

(a) *Work Health and Safety Act 2011*;

(b) *Disaster Management Act 2003*;

(c) *Police Powers and Responsibilities Act 2000*;

(d) *Public Safety Preservation Act 1986*;

(e) *State Transport Act 1938*.

Part 2 Interpretation

7 Definitions

The dictionary in the schedule defines particular words used in this Act.

8 Meaning of *surface transport operation*

(1) A ***surface transport operation*** is an activity or system for—

(a) transporting passengers by high occupancy vehicles; or

(b) transporting goods by high payload vehicles.

(2) In this section—

high occupancy vehicle means a vehicle designed to carry 10 or more seated adults, including the driver.

high payload vehicle means a vehicle with a payload of more than 20t.

9 Meaning of *security-identified surface transport operation* or *SISTO*

A ***security-identified surface transport operation*** or ***SISTO*** is a surface transport operation declared by the chief executive

under section 11 to be a security-identified surface transport operation.

Chapter 2 Declaration of SISTOs

10 Assessment of the level of risk of being a target of a terrorist act

(1) The chief executive may assess the level of risk a surface transport operation has of being a target of a terrorist act.

(2) In carrying out the assessment, the chief executive must take into account relevant information relating to the risk that is—

(a) given to the chief executive by a government agency or an entity carrying on a surface transport operation; or

(b) publicly available.

(3) Without limiting subsection (2), the relevant information may include—

(a) intelligence, including information obtained by a law enforcement agency; and

(b) the following information about the surface transport operation—

- its location
- the type of activities carried on
- the type of goods transported
- its size, including the number of passengers or volume of goods transported.

(4) Also, for the assessment, the chief executive may, in writing, ask the entity carrying on the surface transport operation to give stated relevant information about the surface transport operation to the chief executive within a stated reasonable period.

(5) An entity to whom a request is made under subsection (4) must comply with the request, unless the entity has a reasonable excuse.

Maximum penalty for subsection (5)—60 penalty units.

11 Declaration

(1) The chief executive may declare a surface transport operation to be a security-identified surface transport operation if the chief executive has assessed it under section 10 as having an elevated risk of being the target of a terrorist act.

(2) The declaration must be made by gazette notice (***declaration notice***).

(3) The declaration notice must state the following—

(a) a sufficient identification of the surface transport operation;

(b) that the surface transport operation is declared to be a security-identified surface transport operation;

(c) the name of the entity carrying on the surface transport operation;

(d) any other information the chief executive considers appropriate.

(4) The declaration notice must state a prescribed period as mentioned in section 15(2), definition *prescribed period*, paragraph (a).

(5) It is immaterial for this section and section 10 whether the surface transport operation is part of a larger surface transport operation.

12 Amending a declaration notice

(1) The chief executive may, by gazette notice, amend a declaration notice for a SISTO if the chief executive reasonably believes—

(a) the risks to the SISTO have changed to the extent that the identification of the extent of the SISTO needs to be amended; and

(b) the declaration notice needs to be amended to reflect the change.

(2) The matters the chief executive may have regard to in deciding if there has been a change in the risks to the SISTO include, but are not limited to, the following—

(a) a risk management plan or an amendment of a risk management plan for the SISTO given to the chief executive under chapter 3;

(b) the annual certificate for the SISTO;

(c) intelligence and other relevant information relating to the risks given to the chief executive by a government agency;

Example—

information obtained by a law enforcement agency

(d) other intelligence and information relevant to an assessment of the risks.

13 Giving notice about a declaration to the SISTO entity

(1) After a declaration notice is gazetted for a SISTO, the chief executive must give the SISTO entity written notice stating the following—

(a) a sufficient identification of the SISTO;

(b) the date on which it was declared to be a SISTO;

(c) that the SISTO entity has obligations under this Act.

(2) A notice under subsection (1) must also—

(a) identify each other SISTO (***related SISTO***), if any—

(i) with which the SISTO interacts; or

(ii) that is in close proximity to the SISTO; and

(b) for each related SISTO—state the name of, and contact details for, the related SISTO entity.

(3) If the chief executive amends a declaration notice for a SISTO, the chief executive must give the SISTO entity written notice stating—

(a) how the declaration notice was amended; and

(b) the date on which the amendment was gazetted.

(4) If the chief executive revokes a declaration notice for a SISTO, the chief executive must give the SISTO entity written notice stating—

(a) the declaration notice is revoked; and

(b) the date on which the revocation was gazetted.

(5) Failure to comply with this section does not affect the validity of a gazette notice under section 11, 12 or 14.

14 Revoking a declaration notice

(1) This section applies if the chief executive reasonably believes a SISTO no longer has an elevated risk of being a target of a terrorist act because of either or both of the following—

(a) intelligence or other information relating to the risk and given to the chief executive by a government agency, or that is publicly available, indicates a decrease in the national counter-terrorism alert level or the SISTO's level of risk;

(b) a change in the SISTO's circumstances shown by information given to the chief executive under this Act about the SISTO.

Example of a SISTO's circumstances for paragraph (b)—

a circumstance mentioned in section 10(3)(b)

(2) The chief executive may, by gazette notice, revoke the declaration notice for the SISTO.

Chapter 3 SISTOs

Part 1 Preparing risk management plan

15 Requirement to prepare a risk management plan and give a copy of it to the chief executive

(1) A SISTO entity must—

(a) prepare a risk management plan for the SISTO under this part; and

(b) give a copy of the plan, in written or electronic form, to the chief executive within the prescribed period.

Maximum penalty—60 penalty units.

(2) In this section—

prescribed period, for giving a copy of a risk management plan to the chief executive, means—

(a) if a period of 3 months or longer is stated in the declaration notice for the SISTO for giving the copy—the stated period; or

(b) if paragraph (a) does not apply—the 3 month period after the declaration notice is gazetted.

16 Preparing a plan

(1) A risk management plan must be prepared in accordance with each of the following documents as amended, or remade, from time to time—

(a) an AS/NZS providing for counter-terrorism risk management that is prescribed under a regulation;

(b) to the extent the document mentioned in paragraph (a) does not provide for a matter relating to the preparation

of the risk management plan, AS/NZS ISO 31000:2009 Risk management—Principles and guidelines.

(2) The objectives of the risk management plan are each of the following—

(a) to prevent or reduce the risks to the SISTO of a terrorist act involving the SISTO;

(b) to lessen the effects on the SISTO of a terrorist act involving the SISTO;

(c) to provide for the recovery and continuity of the SISTO in the event of a terrorist act;

(d) to foster communication and cooperation, in relation to counter-terrorism measures, with the following—

(i) if the SISTO has 1 or more related SISTOs—each related SISTO entity;

(ii) the owners or occupiers of areas immediately neighbouring a facility used for carrying on the SISTO.

(3) The risk management plan may comprise an existing plan that complies with section 17 and addresses the threat and consequences of the SISTO being a target of a terrorist act.

Examples of an existing plan for a SISTO—

- an existing security plan
- an existing on-site emergency response plan
- an existing business continuity plan

(4) In this section—

AS/NZS means a standard published jointly by Standards Australia and Standards New Zealand.

17 Content of a plan

(1) A risk management plan for a SISTO must—

(a) contain an assessment of the risks to the SISTO of a terrorist act involving the SISTO; and

(b) state the measures to be taken to prevent or reduce the risks; and

(c) contain a range of measures to respond to changes in the national counter-terrorism alert level or the SISTO's level of risk.

(2) The risk management plan must also state the measures to be taken in the event of a particular security incident involving the SISTO, including the procedures for each of the following—

(a) responding to the security incident;

(b) recovering the SISTO from the security incident;

(c) providing for the SISTO's continuity;

(d) communicating immediately with the Queensland Police Service;

(e) unless otherwise instructed by the chief executive, communicating as soon as practicable with—

(i) the chief executive; and

(ii) if the SISTO has 1 or more related SISTOs—each related SISTO entity; and

(iii) the owners or occupiers of areas immediately neighbouring a facility used for carrying on the SISTO;

(f) coordinating the risk management plan with any relevant—

(i) emergency plan and procedure prepared under the *Work Health and Safety Act 2011*; and

(ii) disaster management plan prepared under the *Disaster Management Act 2003*; and

(iii) potential exercise of power under the *Public Safety Preservation Act 1986*.

(3) The risk management plan must also—

(a) state details, including the frequency, of relevant training to be given to the employees engaged in carrying on the SISTO; and

(b) provide for the keeping of a record of training given to the employees in accordance with the risk management plan.

(4) The risk management plan must clearly identify each person, whether by reference to the person's position or title, who has an obligation to comply with the risk management plan.

(5) The risk management plan must also state the following—

(a) the positions or titles of the persons involved in carrying on the SISTO who are responsible for implementing the risk management plan;

(b) the contact details, in the case of a security incident, for the persons mentioned in paragraph (a);

(c) the measures to be taken for maintaining security of the auditable records for the SISTO.

(6) If the SISTO has 1 or more related SISTOs, the risk management plan must include the arrangements for coordinating the plan with the risk management plans of the related SISTOs.

(7) In this section—

relevant training means training about the procedures to be followed to prevent or respond to a security incident.

18 Guidelines for preparing a risk management plan

(1) The chief executive may make, and give to a SISTO entity, guidelines about the following—

(a) the preparation of a risk management plan;

(b) the matters to be included in a risk management plan.

(2) If the guidelines are inconsistent with a document mentioned in section 16(1), the document mentioned in that subsection prevails to the extent of the inconsistency.

(3) If the guidelines for a matter are consistent with a document mentioned in section 16(1), compliance with the guidelines in relation to the matter is sufficient compliance with section 16(1) to the extent it relates to the matter.

Part 2 Other provisions about plan

19 Implementing and complying with a plan

(1) A SISTO entity must implement the risk management plan for the SISTO as soon as possible after the plan is prepared.

Maximum penalty—50 penalty units.

(2) A SISTO entity must take all reasonable steps to ensure each person who has an obligation to comply with the risk management plan for the SISTO complies with it.

Maximum penalty—50 penalty units.

20 Annual audit of risk management plan

A SISTO entity must conduct an audit each year, not more than 1 year after the previous audit, to check whether the risk management plan for the SISTO is being implemented, and complied with, by the entity's employees.

Maximum penalty—50 penalty units.

21 Audit record

(1) A SISTO entity must keep a record of an audit conducted under section 20 for the SISTO, as required under this section.

Maximum penalty—50 penalty units.

(2) The record must contain the following information—

(a) the date of the audit;

(b) the name of the person (the ***auditor***) who carried out the audit;

(c) the auditor's contact details and, if applicable, the auditor's position or title within an entity responsible for conducting the audit;

(d) the audit results, including the auditor's recommended actions and recommended implementation dates for the actions;

(e) the auditor's recommended actions that have been implemented and the dates on which they were implemented;

(f) the auditor's recommended actions that have not been implemented and the reasons why they have not been implemented.

(3) The record must be kept for 3 years after the date of the last entry in the record.

22 Reviewing a plan

(1) A SISTO entity must review the risk management plan for the SISTO under subsection (2) to check the plan's continued compliance with sections 16 and 17.

Maximum penalty—50 penalty units.

(2) The risk management plan must be reviewed as soon as possible after any of the following happens—

(a) the SISTO entity is given a notice under section 13(3) that the declaration notice for the SISTO has been amended;

(b) the entity becomes aware of a systemic problem with the plan because of an audit of the plan under section 20, or an exercise conducted under section 25 to test the operation of the plan;

(c) the SISTO's circumstances change in a way that may affect the SISTO's level of risk;

(d) a security incident involving the SISTO;

(e) the end of 5 years after the risk management plan was prepared, or last reviewed under this section.

23 Review record

(1) A SISTO entity must prepare and keep a record of a review conducted under section 22 for the SISTO as required under this section.

Maximum penalty—50 penalty units.

(2) The record must be prepared within 28 days after the review ends.

(3) The record must contain the following information—

(a) the date of the review;

(b) the happening mentioned in section 22(2) that caused the review;

(c) the name of the person (the ***reviewer***) who carried out the review;

(d) the reviewer's position or title and the reviewer's relationship to the SISTO;

(e) the review results, including the reviewer's recommended actions and recommended implementation dates for the actions;

(f) the reviewer's recommended actions that have been implemented and the dates on which the actions were implemented;

(g) the reviewer's recommended actions that have not been implemented and the reasons why they have not been implemented.

(4) The record must be kept for 3 years after the date of the last entry in the record.

24 Amending a plan after review

(1) Within 28 days after a SISTO entity becomes aware of a deficiency in the risk management plan for the SISTO, the entity must amend the plan to rectify the deficiency.

Maximum penalty—50 penalty units.

(2) Within 28 days after an amendment is made under subsection (1), the SISTO entity must give a copy of the amendment, or a copy of the plan as amended, to the chief executive.

Maximum penalty—60 penalty units.

(3) In this section—

deficiency, in relation to a risk management plan, means a deficiency in the plan's compliance with section 16 or 17.

25 Preparing, conducting and participating in exercises to test the operation of a plan

(1) A SISTO entity must test the operation of the risk management plan for the SISTO at least once in each year by—

(a) either—

(i) planning and conducting 1 or more exercises complying with the prescribed standard; or

(ii) contributing to the planning and conduct of at least 1 exercise conducted by another entity to test surface transport security plans and arrangements; and

Examples of another entity—

a government agency, another SISTO

(b) taking all reasonable steps to ensure that each person having an obligation under the risk management plan participates in at least 1 exercise that tests the part of the plan relevant to the person's obligation.

Maximum penalty—60 penalty units.

(2) A SISTO entity must also comply with any direction given to the entity by the chief executive to test the operation of the risk management plan for the SISTO by participating in an exercise mentioned in subsection (1)(a)(ii).

Maximum penalty—60 penalty units.

(3) However, subsection (2) does not apply to a SISTO entity if it has already participated in an exercise mentioned in subsection (1)(a)(ii) in relation to the SISTO in the year in which the direction is given.

(4) At least 28 days before an exercise mentioned in subsection (1)(a) is conducted for a SISTO, the SISTO entity must, unless the entity has a reasonable excuse—

(a) give the chief executive a copy of the plan for the exercise; and

(b) tell the chief executive the date and time of the exercise.

Maximum penalty—60 penalty units.

(5) An authorised officer may observe the exercise.

(6) In this section—

prescribed standard means—

(a) a standard prescribed under a regulation; or

(b) if no standard is prescribed—the 'Australian Emergency Manuals Series, part V—The management of training—manual 42—Managing exercises' published by Emergency Management Australia from time to time.

26 Test exercise record

(1) A SISTO entity must prepare and keep a record of each exercise conducted under section 25 involving the SISTO, as required under this section.

Maximum penalty—50 penalty units.

(2) The record must be prepared within 28 days after the exercise ends.

(3) The record must contain the following information—

(a) the date the exercise was conducted;

(b) the name, contact details and position or title in relation to the SISTO entity or other entity of the person who planned and conducted the exercise;

(c) what part of the risk management plan was tested.

(4) The record must be kept for 3 years after the date of the last entry in the record.

27 Annual certificate about auditing, reviewing and testing the operation of the plan

(1) Each year, a SISTO entity must give the chief executive a certificate in the approved form about the risk management plan for the SISTO (***annual certificate***) as required under subsection (2).

Maximum penalty—60 penalty units.

(2) The annual certificate must be signed by or for the SISTO entity and given to the chief executive before the later of the following—

(a) 1 September;

(b) the day stated by the chief executive in a written notice given to the entity.

(3) The approved form must provide for information about the following to be included in the form—

(a) whether there is a risk management plan for the SISTO addressing the threat and consequences of the SISTO being a target of a terrorist act;

(b) the date the plan was prepared;

(c) the information mentioned in section 21(2) about the most recent audit of the plan;

(d) the information mentioned in section 23(3) about the most recent review of the plan;

(e) the information mentioned in section 26(3) about the most recent exercise testing the operation of the plan.

28 Giving chief executive notice of change to contact information in risk management plan

(1) This section applies if a change happens in the information stated in a risk management plan for a SISTO under section 17(5)(a) and (b) (the ***emergency contact information***).

(2) Within 2 business days after becoming aware of the change, the SISTO entity must give written notice of the updated emergency contact information to—

(a) the chief executive; and

(b) if the SISTO has 1 or more related SISTOs—each related SISTO entity.

Maximum penalty—60 penalty units.

Chapter 4 Monitoring and enforcement

Part 1 Authorised officers

29 Appointment and qualifications

(1) The chief executive may appoint any of the following persons as an authorised officer—

(a) an officer of the department;

(b) another person decided by the chief executive.

(2) However, the chief executive may appoint a person as an authorised officer only if the chief executive is satisfied the

person is qualified for appointment because the person has the necessary expertise or experience.

30 Appointment conditions and limit on powers

(1) An authorised officer holds office on any conditions stated in—

(a) the authorised officer's instrument of appointment; or

(b) a signed notice given to the authorised officer; or

(c) a regulation.

(2) The instrument of appointment, a signed notice given to the authorised officer or a regulation may limit the authorised officer's powers under this Act.

(3) In this section—

signed notice means a notice signed by the chief executive.

31 Issue of identity card

(1) The chief executive must issue an identity card to each authorised officer.

(2) The identity card must—

(a) contain a recent photo of the authorised officer; and

(b) contain a copy of the authorised officer's signature; and

(c) identify the person as an authorised officer under this Act; and

(d) state an expiry date for the card.

(3) This section does not prevent the issue of a single identity card to a person for this Act and other purposes.

32 Production or display of identity card

(1) In exercising a power under this Act in relation to a person, an authorised officer must—

(a) produce the authorised officer's identity card for the person's inspection before exercising the power; or

(b) have the identity card displayed so it is clearly visible to the person when exercising the power.

(2) However, if it is not practicable to comply with subsection (1), the authorised officer must produce the identity card for the person's inspection at the first reasonable opportunity.

(3) For subsection (1), an authorised officer does not exercise a power in relation to a person only because the authorised officer has entered a place as mentioned in section 36(1)(b) or (3).

33 When authorised officer ceases to hold office

(1) An authorised officer ceases to hold office if any of the following happens—

(a) the term of office stated in a condition of office ends;

(b) under another condition of office, the authorised officer ceases to hold office;

(c) the authorised officer's resignation under section 34 takes effect.

(2) Subsection (1) does not limit the ways an authorised officer may cease to hold office.

(3) In this section—

condition of office means a condition on which the authorised officer holds office.

34 Resignation

An authorised officer may resign by signed notice given to the chief executive.

35 Return of identity card

A person who ceases to be an authorised officer must return the person's identity card to the chief executive within 7 days after ceasing to be an authorised officer, unless the person has a reasonable excuse.

Maximum penalty—10 penalty units.

Part 2 Powers of authorised officers

Division 1 Entry of places

36 Power to enter places

(1) An authorised officer may enter a place if—

(a) an occupier of the place consents to the entry; or

(b) it is a public place and the entry is made when it is open to the public.

(2) Also, an authorised officer may enter a place occupied by a SISTO entity—

(a) to observe an exercise under section 25(5); or

(b) subject to subsection (5), to check that the risk management plan for the SISTO is being implemented and complied with.

(3) For the purpose of asking an occupier of a place for consent to enter, an authorised officer may, without the occupier's consent—

(a) enter land around premises at the place to an extent that is reasonable to contact the occupier; or

(b) enter part of the place the authorised officer reasonably considers members of the public ordinarily are allowed to enter when they wish to contact the occupier.

(4) For subsections (2) and (3), a place does not include a part of the place where a person resides.

(5) An authorised officer may enter a place under subsection (2)(b) only if the SISTO entity occupying the place has been given at least 7 days written notice of the intended entry and its purpose.

37 Procedure for entry with consent

(1) This section applies if an authorised officer intends to ask an occupier of a place to consent to the authorised officer or another authorised officer entering the place under section 36(1)(a).

(2) Before asking for the consent, the authorised officer must tell the occupier—

(a) the purpose of the entry; and

(b) that the occupier is not required to consent.

(3) If the consent is given, the authorised officer may ask the occupier to sign an acknowledgment of the consent.

(4) The acknowledgment must state—

(a) the occupier has been told—

(i) the purpose of the entry; and

(ii) that the occupier is not required to consent; and

(b) the purpose of the entry; and

(c) the occupier gives the authorised officer consent to enter the place and exercise powers under this part; and

(d) the time and date the consent was given.

(5) If the occupier signs the acknowledgment, the authorised officer must immediately give a copy to the occupier.

(6) If—

(a) an issue arises in a proceeding about whether the occupier consented to the entry; and

(b) an acknowledgment complying with subsection (4) for the entry is not produced in evidence;

the onus of proof is on the person relying on the lawfulness of the entry to prove the occupier consented.

Division 2 Entry of prescribed vehicles

38 Power of entry

(1) An authorised officer may enter a prescribed vehicle if the authorised officer reasonably believes the entry is necessary for the authorised officer—

(a) to observe an exercise under section 25(5); or

(b) to check that the risk management plan for a SISTO is being implemented and complied with.

(2) However, before an authorised officer enters a prescribed vehicle under subsection (1)(b), an authorised officer must have given the owner of the vehicle at least 7 days written notice of the intended entry and its purpose.

39 Procedure before entry

(1) This section applies if an authorised officer intends to enter a prescribed vehicle under section 38.

(2) If a person is present at the prescribed vehicle, the authorised officer must, before entering the prescribed vehicle, do or make a reasonable attempt to do the following things—

(a) comply with section 32;

(b) tell the person the purpose of the entry;

(c) ask for the person's consent to the entry;

(d) tell the person the authorised officer is permitted under this Act to enter the prescribed vehicle without consent.

(3) If a person is not present at the prescribed vehicle, the authorised officer must, before entering the prescribed vehicle—

(a) take reasonable steps to find the owner of the prescribed vehicle; and

(b) comply with subsection (2)(a) to (d) for the owner.

(4) Subsection (3) does not require the authorised officer to take a step the authorised officer believes may frustrate or otherwise hinder the purpose of the intended entry.

(5) In this section—

owner, of a prescribed vehicle, includes a person who appears to be in control of the prescribed vehicle.

Division 3 General enforcement powers

40 Application of div 3

(1) This division applies to an authorised officer who may enter, or has entered, a place under division 1 or a prescribed vehicle under division 2.

(2) However, if an authorised officer, under section 36(3), enters a place to ask the occupier's consent to enter premises, this division applies to the authorised officer only if the consent is given or the entry is otherwise authorised.

41 General powers of authorised officer after entering a place or prescribed vehicle

For monitoring or enforcing compliance with this Act, the authorised officer may do any of the following—

(a) inspect, film, measure, photograph, videotape or otherwise record an image of anything at the place or in or on the prescribed vehicle;

(b) take an extract from, or copy, a document at the place or in the prescribed vehicle;

(c) take into the place or prescribed vehicle the equipment, materials or persons the officer reasonably requires for exercising a power under this part;

(d) take a necessary step to allow a power under paragraphs (a) to (c) to be exercised.

42 Power to require reasonable help or information

(1) An authorised officer may require a relevant person at a place or prescribed vehicle entered under this part to give the authorised officer—

(a) reasonable help to exercise a power under section 41; or

Examples of a requirement for paragraph (a)—

- a requirement to give the authorised officer reasonable help to find and gain access to a particular document required to be kept under this Act
- a requirement to operate electronic equipment at the place to enable the authorised officer to copy a document on a disk, tape or other device

(b) information, including electronically stored information, to help the authorised officer ascertain whether this Act is being or has been complied with.

Note—

See also, section 45(1)(a) for an authorised officer's further power to require information.

(2) When making a requirement under subsection (1), the authorised officer must warn the person that it is an offence to fail to comply with the requirement unless the person has a reasonable excuse.

(3) A person required to give reasonable help under subsection (1)(a), or to give information under subsection (1)(b), must comply with the requirement, unless the person has a reasonable excuse.

Maximum penalty—60 penalty units.

(4) If the person is an individual, it is a reasonable excuse for the person not to comply with a requirement to give information

under subsection (1)(b) if complying with the requirement might tend to incriminate the person or make the person liable to a penalty.

(5) In this section—

relevant person means—

(a) for a place—the occupier of, or someone else at, the place; or

(b) for a prescribed vehicle—the person in control of, or someone else at, the prescribed vehicle.

Division 4 Other powers

43 Power to require a name and address

(1) This section applies if an authorised officer—

(a) finds a person committing an offence against this Act; or

(b) finds a person in circumstances that lead the authorised officer reasonably to suspect the person has committed an offence against this Act; or

(c) has information that leads the authorised officer reasonably to suspect a person has just committed an offence against this Act.

(2) The authorised officer may require the person to state the person's name and residential or business address.

(3) When making the requirement, the authorised officer must warn the person it is an offence to fail to state the person's name or residential or business address, unless the person has a reasonable excuse.

(4) The authorised officer may also require the person to give the authorised officer evidence of the correctness of the stated name or address if the authorised officer reasonably suspects the stated name or address to be false.

44 Failure to give a name or address

(1) A person of whom a requirement is made under section 43(2) or (4) must comply with the requirement, unless the person has a reasonable excuse.

Maximum penalty—40 penalty units.

(2) A person does not commit an offence against subsection (1) if—

(a) the person was required to state the person's name or residential or business address by an authorised officer who suspected the person had committed an offence against this Act; and

(b) the person is not proved to have committed the offence.

(3) If the person is an individual, it is a reasonable excuse for the person to fail to comply with the requirement that complying with the requirement might tend to incriminate the person or make the person liable to a penalty.

45 Power to require information or documents

(1) For monitoring or enforcing compliance with this Act, an authorised officer may require a person to—

(a) give to the authorised officer, either orally or in writing, information in the person's knowledge about a stated matter within a stated reasonable time and in a stated reasonable way; or

(b) give to the authorised officer, within a stated reasonable time and in a stated reasonable way, a document about a stated matter in the person's possession or control.

Example—

information or a document about the preparation, implementation, auditing, reviewing or testing of the operation of the risk management plan

(2) The authorised officer may keep a document mentioned in subsection (1)(b) to copy it.

(3) The authorised officer must return the document to the person as soon as practicable after copying it.

(4) A person of whom a requirement is made under subsection (1) must comply with the requirement, unless the person has a reasonable excuse.

Maximum penalty—60 penalty units.

(5) If the person is an individual, it is a reasonable excuse for the person to fail to comply with a requirement made under subsection (1) that complying with the requirement might tend to incriminate the person or make the person liable to a penalty.

(6) If a court convicts a person of an offence against subsection (4), the court may also order the person to give to the chief executive or a stated authorised officer, within a stated time and in a stated way, information or a document to which the requirement related.

Chapter 5 Powers of chief executive

46 Power to give a direction to comply

(1) If a SISTO entity fails to comply with a prescribed provision, the chief executive may, in writing, direct the entity to comply with the prescribed provision within the period stated in the direction.

(2) The SISTO entity must comply with the direction, unless the entity has a reasonable excuse.

Maximum penalty—

(a) if the direction is about compliance with section 19, 20, 22(1) or 24(1)—500 penalty units; or

(b) otherwise—60 penalty units.

(3) In this section—

prescribed provision means section 15(1), 19, 20, 22(1), 24(1), 25(1) or (2), 27(1) or 28(2).

47 Power to seek a court order suspending SISTO if there is an unacceptable risk of significant adverse impacts

(1) The chief executive may apply to the Supreme Court for an order under this section on the grounds mentioned in subsection (2).

(2) For subsection (1) the grounds are that, because of a SISTO entity's persistent or repeated contravention of 1 or more provisions of this Act, the SISTO's continued operation presents an unacceptable risk of significant adverse impacts relating to the SISTO associated with a terrorist act involving the SISTO.

(3) The application may not be made unless the SISTO entity has been convicted at least once for a contravention of this Act, regardless of when the contravention or conviction happened in relation to any other contravention relied on.

(4) The application must state each of the following—

(a) each contravention of this Act that is relied on;

(b) the particulars of the SISTO entity's alleged persistent or repeated contravention of this Act.

(5) The Supreme Court may make an order under this section if satisfied that the SISTO's continued operation presents an unacceptable risk of significant adverse impacts relating to the SISTO associated with a terrorist act involving the SISTO.

(6) The order may include an order suspending all or part of the SISTO until a stated day, for a stated period or until stated action has been taken.

Example of stated action—

an amendment of the risk management plan for the SISTO to lessen a new risk of a terrorist act being carried out involving the SISTO

Chapter 6 Other enforcement matters

48 False or misleading statements

(1) A person must not state anything to the chief executive or an authorised officer that the person knows is false or misleading in a material particular.

Maximum penalty—60 penalty units

(2) It is enough for a complaint for an offence against subsection (1) to state the statement made was 'false or misleading' to the person's knowledge, without specifying which.

49 False or misleading documents

(1) A person must not give the chief executive or an authorised officer a document containing information the person knows is false or misleading in a material particular.

Maximum penalty—60 penalty units.

(2) Subsection (1) does not apply to a person who, when giving the document to the chief executive or authorised officer—

(a) informs the chief executive or authorised officer, to the best of the person's ability, how it is false or misleading; and

(b) gives the correct information to the chief executive or authorised officer if the person has, or can reasonably obtain, the correct information.

(3) It is enough for a complaint for an offence against subsection (1) to state the document given was 'false or misleading' to the person's knowledge, without specifying which.

50 Obstructing an authorised officer

(1) A person must not obstruct an authorised officer in the exercise of a power under this Act, unless the person has a reasonable excuse.

Maximum penalty—60 penalty units.

(2) If a person has obstructed an authorised officer under subsection (1) and the authorised officer decides to exercise the power, the authorised officer must, if practicable, warn the person—

(a) that the authorised officer considers the person's conduct is obstructing the authorised officer; and

(b) that it is an offence to obstruct the authorised officer unless the person has a reasonable excuse.

(3) In this section—

obstruct includes abuse, hinder, insult, intimidate, resist and threaten and attempt to obstruct.

51 Pretending to be an authorised officer

A person must not pretend to be an authorised officer.

Maximum penalty—80 penalty units.

Chapter 7 Legal proceedings

52 Proceedings for offences

(1) An offence against this Act is a summary offence.

(2) A proceeding for an offence must start—

(a) within 1 year after the commission of the offence; or

(b) within 6 months after the offence comes to the complainant's knowledge, but within 2 years after the commission of the offence.

(3) A statement in a complaint for an offence against this Act that the matter of the complaint came to the knowledge of the complainant on a stated day is evidence of when the matter came to the complainant's knowledge.

53 Court may prohibit publication of all or part of a proceeding

(1) The court may make the orders it considers appropriate to prohibit the publication of all or any part of a proceeding under this Act.

Example—

an order that the proceeding be heard in closed court

(2) Subsection (1) does not limit the orders the court may make.

54 Protection of counter-terrorism information in legal proceedings

(1) This section applies if, in a proceeding before a court or tribunal, an issue arises relating to the disclosure of counter-terrorism information and, but for this section, a person would be entitled to require another person to disclose the information.

(2) The court or tribunal may excuse the other person from the requirement to disclose if satisfied—

(a) that—

(i) disclosure is likely to prejudice the prevention, investigation or prosecution of a terrorist act or suspected terrorist act; or

(ii) disclosure is not permitted under the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cwlth); or

(iii) under the *Police Powers and Responsibilities Act 2000*, section 803, a police officer would not be required to disclose the information; and

(b) the public interest in preserving secrecy or confidentiality outweighs the public interest in disclosure.

56 Inclusion of reasonable diligence

For a provision of this Act that provides that a SISTO entity may avoid liability for an offence by proving the entity took all reasonable steps in relation to a matter, the taking of all reasonable steps includes the exercise of reasonable diligence.

Chapter 8 Miscellaneous

57 Confidentiality

(1) A person must not disclose, record or use information the person gained—

(a) through involvement in the administration of this Act; or

(b) because of an opportunity provided by the involvement.

Maximum penalty—200 penalty units.

(2) However, a person may disclose, record or use the information—

(a) in the discharge of a function under this Act; or

(b) if it is authorised—

(i) under another Act or a regulation; or

(ii) by the person to whom the information relates; or

(c) in a proceeding before a court or tribunal in which the information is relevant.

(3) In this section—

disclose information means—

(a) intentionally or recklessly disclose the information; or

(b) allow access to the information.

58 Protection from liability

(1) An official is not civilly liable for an act done, or omission made, honestly and without negligence under this Act.

(2) If subsection (1) prevents a civil liability attaching to an official, the liability attaches instead to the State.

(3) In this section—

official means—

(a) the Minister; or

(b) the chief executive; or

(c) an authorised officer, other than a person appointed as an authorised officer under section 29(1)(b) who is not a public service employee; or

(d) a public service employee; or

(e) a person acting under the direction of a person mentioned in any of paragraphs (a) to (d).

59 Approved forms

The chief executive may approve forms for use under this Act.

60 Regulation-making power

(1) The Governor in Council may make regulations under this Act.

(2) Without limiting subsection (1), a regulation may prescribe offences for a contravention of a regulation and fix a maximum penalty of not more than 20 penalty units for a contravention.

61 Reviews of Act

(1) The Minister must review this Act every 5 years to decide whether its provisions remain appropriate.

(2) The first review must be carried out as soon as practicable after 12 December 2018.

(3) Each subsequent review must be carried out as soon as practicable after each fifth anniversary of the date mentioned in subsection (2).

(4) The Minister must, for each review carried out under this section, table a report on the review's outcome in the Legislative Assembly—

(a) as soon as practicable after the review is carried out; and

(b) in any event, within 1 year after the end of the 5-year period for which the review is carried out.

Schedule Dictionary

section 7

annual certificate see section 27(1).

auditable record, for a SISTO, means the following for the SISTO—

(a) the risk management plan;

(b) the audit record mentioned in section 21;

(c) the review record mentioned in section 23;

(d) the test exercise record mentioned in section 26;

(e) the training record required to be kept in accordance with the risk management plan.

conviction includes a finding of guilt, and the acceptance of a plea of guilty, by a court, whether or not a conviction is recorded.

declaration notice see section 11(2).

elevated risk, of being the target of a terrorist act, for a surface transport operation, means the surface transport operation has a greater risk of being a target of a terrorist act than other surface transport operations generally.

entity, carrying on a surface transport operation, SISTO or related SISTO, means the person that is—

(a) the owner or operator of the surface transport operation, SISTO or related SISTO; or

(b) if the owner or operator has appointed a managing agent to carry on the surface transport operation, SISTO or related SISTO—the managing agent.

government agency includes—

(a) the State, the Commonwealth or another State; or

(b) an agency of the Commonwealth or a State.

high occupancy vehicle see section 8(2).

high payload vehicle see section 8(2).

intelligence means the product resulting from the collection, evaluation, analysis, integration and interpretation of all available information relating to 1 or more aspects of terrorist activity.

law enforcement agency includes the following—

(a) the Australian Federal Police;

(b) a police force or service of another State;

(c) a department of government, agency, authority, commission, instrumentality, office, or other entity of any State or the Commonwealth established for a law enforcement or counter-terrorism purpose;

(d) a part of an entity mentioned in paragraph (c);

(e) an officer, employee or member of an entity mentioned in any of paragraphs (a) to (d).

level of risk, of a SISTO, means the level of risk the SISTO has of being a target of a terrorist act.

national counter-terrorism alert level means the current level of alert for Australia of a terrorist act being carried out as published by the Australian Government.

plan means a risk management plan.

prescribed vehicle means a high occupancy vehicle or a high payload vehicle.

reasonably believes means believes on grounds that are reasonable in the circumstances.

reasonably considers means considers on grounds that are reasonable in the circumstances.

reasonably suspects means suspects on grounds that are reasonable in the circumstances.

related SISTO see section 13(2).

related SISTO entity means an entity carrying on a related SISTO.

risk management plan means a risk management plan under chapter 3.

risks, to a SISTO, include risks to—

(a) persons, equipment and facilities used in carrying on the SISTO; and

(b) passengers or goods transported by use of the SISTO.

security-identified surface transport operation see section 9.

security incident means—

(a) a terrorist act; or

(b) another incident that threatens the security of a SISTO or another surface transport operation against a terrorist act; or

Examples—

- an explosion, or bridge collapse, that is not immediately attributable to a terrorist act
- a change in the national counter-terrorism alert level or a level of risk
- security measures have been tampered with

(c) the threat of a security incident mentioned in paragraph (b).

SISTO see section 9.

SISTO entity means an entity carrying on a SISTO.

surface transport operation see section 8.

terrorist act has the meaning given in the *Police Powers and Responsibilities Act 2000*.

vehicle includes a barge, ferry and train.