Transport Security (Counter-Terrorism) Bill 2008

Explanatory Notes

Short Title

The short title of the Bill is the Transport Security (Counter-Terrorism) Bill 2008.

Policy Objectives of the Legislation

The Bill is a significant community and transport initiative to provide for the increased preparedness of surface transport operations against the adverse impacts of an act or threat of terrorism.

In keeping with the philosophy of applying resources on a risk basis, the Bill focuses on surface transport operations that are at an 'elevated risk,' and provides for identifying those operations as security-identified surface transport operations (SISTOs).

The Bill introduces a regulatory framework and tools to promote compliance by SISTOs. The regulatory regime provides that counter-terrorism preparedness measures are established and maintained through the development and implementation of risk management plans. Further, it also puts into place mechanisms for those plans to remain valid and compliant.

The legislation also provides government with assurance that surface transport operations are prepared for the adverse risk of terrorism through an annual certificate.

This legislation is not designed to prevent a terrorist act or threat, but ensures that SISTOs have considered the risk of terrorism to their operation and mitigated this risk accordingly. Further, the Bill does not supersede the powers or responsibility accorded to law enforcement agencies under the *Police Powers and Responsibilities Act 2000* and the *Public Safety Preservation Act 1986*.

Reasons for the Bill

The Bill focuses on strengthening the preparedness and resilience of certain Queensland surface transport operations against terrorism. Current legislation does not provide for increasing the preparedness of surface transport operations from an act or threat of terrorism.

This legislation will provide government and the community with a proportionate level of assurance that surface transport operations that have been assessed as having an elevated risk have appropriately considered the protection of their operation.

It is widely recognised across jurisdictions and internationally that legislation is an appropriate vehicle for ensuring counter-terrorism arrangements in the transport industry.

In London (July 2005), Madrid (March 2004) and Mumbai (July 2006), terrorists have demonstrated the capacity and intent to attack surface transport systems, killing innocents and causing social and economic disruption.

In London especially, following the attacks on bus and rail services, mechanisms have been put in place to ensure that transport services have plans to mitigate the risk of terrorism and also ensure that those plans are tested regularly with exercises.

This legislation will also significantly progress Queensland's responsibilities under the *Intergovernmental Agreement on Surface Transport Security* (the Intergovernmental Agreement), approved by the Council of Australian Governments (COAG) on 3 June 2005. The Intergovernmental Agreement outlined that states and territories are responsible for identifying SISTOs and for ensuring that those operations develop and implement preventative security measures. In the counter-terrorism context, states and territories have primary responsibility for surface transport security for buses, trains, ferries, freight and associated infrastructure.

As a signatory to the Intergovernmental Agreement, Queensland is responsible for increasing the protective security, planning and preventative measures in the surface transport system. Further, the agreement also provides that the parties will review their legislative arrangements to make sure that they are sufficiently strong in support of the purpose; securing transport from terrorism. The Bill provides for meeting these

responsibilities with a regulatory regime focused on developing, implementing and maintaining risk management plans.

The Bill is consistent with other measures in the national transport industry. Similar risk-based approaches to security have been adopted by the Commonwealth Government for aviation and maritime security. The *Maritime Transport and Offshore Facilities Security Act 2003* and the *Aviation Transport Security Act 2004* requires transport operators to generate plans to address and mitigate security risks.

State initiatives to counter-terrorism are outlined under the *Queensland Government Counter-Terrorism Strategy.* Queensland Transport is committed to strengthening protective security arrangements across all transport systems, particularly mass transit and mass freight surface transport systems. Queensland Transport will meet part of this obligation through this Bill, as it will result in surface transport operations that are at an 'elevated risk' of terrorism, having an increased preparedness for an act or threat of terrorism.

How the policy objectives will be achieved

The policy objectives are achieved by increasing the preparedness of SISTOs for an act or threat of terrorism by:

- providing for the assessment of risk to surface transport operations from terrorism;
- providing for the declaration of a security identified surface transport operation;
- ensuring a SISTO undertakes a risk assessment;
- addressing their risk through the preparation of a risk management plan;
- providing for the implementation of the risk management plan to mitigate risk;
- providing for audits and reviews to ensure valid and compliant plans;
- introducing an annual exercise to test the operation of the risk management plan;
- providing for cooperation on counter-terrorism preparedness between related SISTOs;
- establishing information offences to verify compliance;

- introducing an inspection regime to ensure that obligations are being met under the Bill; and
- providing powers to the chief executive, Queensland Transport, to direct SISTOs to comply with provisions under the Bill.

The Bill is complimented by the *Queensland Plan for the Protection of Surface Transport Operations from Terrorism* (the Plan). The Plan, which sits under the *Queensland Government Counter-Terrorism Strategy*, fulfils the vision of a State 'well prepared to prevent, or to act in the event of, a terrorist threat or incident to minimise the impacts on communities.'

The Plan outlines Queensland's approach to the protection of surface transport operations from the threat and consequences of terrorism. The Plan and the Bill, aim to reduce the risk of harm caused by an act or threat of terrorism on Queensland's surface transport system. All surface transport operations, or non-SISTOs, will be provided with guidance material, on request, to assist these operations to integrate counter-terrorism preventative measures as a part of their normal business.

Alternative Ways of Achieving the Policy Objectives

An alternative way of achieving the policy objectives of the Bill could be provided under an unregulated, collaborative approach with industry to produce risk assessments and risk management plans. This is the approach the State has adopted to protect critical infrastructure. There are a number of reasons however, why a legislative regime has been established for transport.

The *Intergovernmental Agreement* required signatories to review supporting legislative arrangements to provide assurances of the preparedness of SISTOs into the future. There is a national emphasis on ensuring that jurisdictions have sufficient legislative strength to protect the community and surface transport operations.

Transport operators in Queensland are already a highly regulated industry to ensure the safety of the traveling public.

World events have highlighted the intent and capability of terrorists to attack surface-based transport systems. These attacks have demonstrated the vulnerability of transport systems to terrorism.

There are a wide variety of organisations that operate transport, from small self-owned operators to large multi-national operations. The Bill will

provide an impetus for all SISTOs, irrespective of their size, to invest resources into counter-terrorism preparedness in the longer-term.

Estimated administrative costs

The implementation of this Bill will result in administrative costs for Queensland Transport and will be, in the current threat environment, absorbed within existing budget allocations. In the event of a terrorist attack, or, in the event that a whole-of-government decision is made to significantly increase counter-terrorism measures (for example, the introduction of security guards) these costs would be subject to separate consideration.

Fundamental Legislative Principles (FLPs)

The Bill has been drafted with due regard to fundamental legislative principles (FLPs) as outlined in the *Legislative Standards Act 1992*. However, the Bill contains three potential breaches of fundamental legislative principles. These breaches are considered essential in the public interest, having regard to the potential impacts of a terrorist act on public safety.

A fundamental legislative principle is not a mandatory or entrenched statutory requirement which would preclude the Parliament from enacting a law which is incompatible with that principle. Further, a fundamental legislative principle does not operate and cannot operate so as to deny validity to an exercise of legislative power in the form of a privative clause.

***Adversely affect rights and liberties or impose obligations retrospectively* (sections 4(2) and 4(3)(g) *Legislative Standards Act 1992*)**

Legislation should not adversely affect rights and liberties without adequate justification. The Bill provides for the development and implementation of a risk management plan and that all persons under that plan fulfil their obligations. Under clause 43, an authorised officer has the power to require a name or address. This power is required by an authorised officer to determine and identify individuals who have obligations under the risk management plans. In the absence of this provision, it would be impossible for an authorised officer to verify a SISTOs compliance with clauses 15 and 19 to 28. Such information is vital to prosecuting non-compliance under the Bill and requiring identification establishes a record in order to ascertain if persons have fulfilled their obligations under the Bill.

Appropriateness of penalties for offences **(section 4(2)(a)** ***Legislative Standards Act 1992*****)**

The *Legislative Standards Act 1992* recognises that penalties should be proportionate to the offence. The Bill introduces new offences for which penalties are provided.

The Bill provides for breaches of the regulation to incur penalties of up to $37,500 (500 penalty units) for clause 46. Specifically, this offence relates to the escalation in penalties in the regulatory regime.

Under the Bill, failure to develop, implement and act on counter-terrorism measures, or risk management plans, may result in mass casualties, significant capital loss or infrastructure damage from one incident, or coordinated incidents. This power provides the chief executive to direct operations that are remaining non-compliant to comply.

The benefits that the Bill will deliver to the community are an increase preparedness of a surface transport operation from the adverse impact of terrorism. These benefits are negated if there is non-compliance. The penalties for non-compliance with these key clauses are set at a level that is commensurate with the consequences to the community of non-compliance.

This maximum penalty of 500 units is proportionate with similar regulatory offences in Queensland legislation involving death or injury. Failure to employ counter-measures in the work environment to ensure workers health and safety has a maximum penalty of 800 penalty units ($60,000) or two years imprisonment under the *Work Health Safety Act 1995* clause 24(1). Under the *Dangerous Goods Safety Management Act 2001*, after determining the "acceptable level of risk" in relation to safe management of dangerous goods, a person who has a safety obligation must discharge the obligation. For failing to discharge their obligation a person is liable for 500 units. However, if the failure to discharge the obligation results in property or environmental damage the maximum penalty is 750 units ($56,250) or 6 months imprisonment. Further, if multiple deaths are caused the penalty is increased to a maximum of 3000 units ($225,000) or 3 years imprisonment.

Likewise, 500 penalty units is less than what is provided under the Victorian *Terrorism (Community Protection) Act 2003*. Part 6 of this Act contains a penalty for non-compliance in the case of a natural person of 600 penalty units ($62,886) maximum and in the case of a body corporate 3000 penalty units ($314,430) maximum.

The penalties provided in this Bill are deemed sufficient to deter non-compliance. The number of penalty units reflects the seriousness of the potential consequences of a contravention in regard to a lack of preparedness against an act or threat of terrorism.

Reversing onus of proof **(section 4(3)(d)** ***Legislative Standards Act 1992*****)**

Legislation should not reverse the onus of proof in criminal proceedings without adequate justification. Clause 55 of the Bill may breach this principle. Specifically, clause 55 requires that executive officers ensure surface transport operations comply with the proposed requirements of the Bill. If a transport company commits an offence against a provision, the company's executive officers are taken to have committed the offence of failing to ensure compliance.

This Clause is considered essential to ensure executive officers, those most likely to have knowledge and access to information about the structure, operations and distribution of responsibilities in a company, can be held accountable for any failure to comply with the proposed requirements.

If the prosecution were required to prove an executive officer had committed an offence, obtaining the evidence necessary to prove liability would add cost and cause delay in an environment where certainty and immediate compliance is essential if surface transport operations are to be adequately prepared against the adverse impacts of an act or threat of terrorism. This is because the information necessary to prove this defence will be within the defendant's knowledge rather than the prosecutor's, and would be difficult for the prosecution to obtain and prove.

The reversal of the onus of proof is balanced by the fact that the Bill does not include warrant, entry and search powers and that a "reasonable steps defence" is available to executive officers. That is, it will be a defence for an executive officer to prove they exercised reasonable diligence to ensure compliance or that they were not in a position to influence the conduct of the company.

Consultation

Government

The following Government agencies were consulted in the development of this legislation: Department of the Premier and Cabinet; Department of Justice and Attorney-General; Queensland Treasury; Department of Emergency Services; Queensland Police Service; Department of Tourism, Regional Development and Industry; Department of Employment and Industrial Relations; Department of Local Government and Main Roads; Department of State Development, Trade and Innovation.

Industry

Extensive consultation was undertaken with industry groups. Representatives from Queensland Rail, Brisbane Transport, ferry operations operating out of the Port of Cairns, transport places (such as Roma Street Station and Transit Centre and the Cairns Port Authority), freight operations (such as Pacific National) were consulted. Industry bodies including the Queensland Bus Industry Council, Queensland School Bus Alliance, Transport Workers Union and the Property Council were also consulted.

Purpose and Intended Operation of Each Clause

Chapter 1 Preliminary

Part 1 General

Clause 1 sets out the short title of the Bill as the *Transport Security (Counter-Terrorism) Act 2008*.

Clause 2 provides that the Bill will commence on a day to be fixed by proclamation.

Clause 3 sets out the purpose of the Bill which is to provide for the development and implementation of plans for the reduction of risk to security-identified surface transport operations (SISTOs) and their users against significant adverse impacts from terrorist attacks.

Sub-section (2) provides that the purpose is achieved by declaring particular surface transport operations as SISTOs; establishing a regulatory framework for the preparation, implementation and review of risk management plans; and establishing recovery and continuity plans.

Clause 4 provides objectives with regard to the application of the Bill.

Clause 5 confirms that the Bill applies to all persons including the State and Government Owned Corporations, and as far as the Queensland legislative powers permit, other States and the Commonwealth. A State or the Commonwealth is not liable to be prosecuted for an offence under the Bill, although the Bill applies to the State and the Commonwealth in other respects.

Clause 6 states that this Bill is in addition to, and does not limit the *Disaster Management Act 2003*; *Dangerous Goods Safety Management Act 2001*; *Police Powers and Responsibilities Act 2000*; *Public Safety Preservation Act 1986*; and *State Transport Act 1938*. These acts have a role in either planning for hazards that are similar or may include terrorist acts. Further, they provide powers in anticipation or response to a terrorist threat or act.

Part 2 Interpretation

Clause 7 states that the dictionary in the schedule contains the definitions of particular words used in the Bill.

Clause 8 defines the term "surface transport operation", "high occupancy vehicle" and "high payload vehicle".

Clause 9 defines the term "security-identified surface transport operation".

Chapter 2 Declaration of SISTOs

Clause 10 allows the chief executive to assess a surface transport operation's level of risk. The chief executive may take into account various criterion for the determination of risk. The criteria will provide the basis for the determination of surface transport operations which will have obligations under this Bill. However, flexibility will be retained by the chief executive being able to amend the criteria, in accordance with changes in the threat environment. The nature of the terrorist threat is that it is unpredictable and effective management of this threat can change quickly.

Sub-section (2) requires the chief executive to take into account relevant information related to the risk of a surface transport operation. This information may be provided by government agencies to the chief executive from time to time or from the surface transport operation or that is publicly available.

Sub-section (3) states what information the chief executive may take into account in assessing a surface transport operation.

Sub-section (4) enables the chief executive to ask surface transport operations in writing to give relevant information that may inform the assessment of the level of risk to a surface transport operation. It is important that the chief executive is able to ensure that assessment information is accurate in declaring SISTOs. The assessment will also take relative information into account, that is, the risk of one operation relative to another.

Sub-section (5) requires the surface transport operation to comply with the request. It prescribes the maximum penalty that can be imposed for a breach of this provision.

Clause 11 enables the chief executive to declare a surface transport operation assessed at an ‘elevated risk’ as a security-identified surface transport operation (SISTO).

Sub-section (2) requires the chief executive to provide the declaration by gazette notice. This provides a public record of declaration and provides the date of commencement of regulation of the SISTO. Once declared, the SISTO comes under the regulatory regime.

Sub-section (3) requires that the notice must provide: sufficient identification of the SISTO; that the operation is to be declared; the name of the entity carrying on the operation; and any other information considered appropriate.

Sub-section (4) requires that the notice must state the prescribed period as mentioned in section 15(2).

Sub-section (5) provide for surface transport operations that are part of a large organization.

Clause 12 provides for the chief executive to amend a declaration notice to reflect the change in operation or in the wider threat environment.

Sub-section (1) allows the chief executive to amend the declaration notice by gazette notice if the chief executive reasonably believes that a SISTOs local level of risk has changed since the gazetted declaration.

Sub-section (2) states the matters the chief executive may have regard to in deciding a change in the SISTO's level of risk. The local level of risk may be determined by information provided by either the SISTOs or from government on both the general and transport environments.

SISTOs may provide surface transport operation-specific risk information which may be included in the risk management plan or annual certificate. Risk may be altered through the addition of a new rail line; or the addition or removal of the transportation of freight; or an increase or decrease in the targeting of transport by terrorists.

The chief executive may also have regard to intelligence or information given by government agencies.

Clause 13 requires that after declaration, the chief executive must give the SISTO written notice that states sufficient identification of the SISTO; that is to be declared; the date the declaration notice takes effect; and the obligations imposed under the Bill.

Sub-section (2) requires the notice to state the proximity or interaction of the SISTO to other related SISTOs. It must provide the name and contact details of the entity carrying on the related SISTO. This ensures that SISTOs are aware of the risks posed by other SISTOs and ensures that they have the appropriate information, such as contact details, in order to coordinate risk management plans.

Sub-sections (3) and (4) provides that if the chief executive amends or revokes the declaration notice, the chief executive must give written notice

stating how the notice was amended and the date on which the amendment was gazetted; or written notice stating how the notice was revoked and the date on which the revocation was gazetted.

Sub-section (5) states that failure to comply with this provision does not affect the validity of a gazette notice under clauses 11, 12, or 14.

Clause 14 provides for the chief executive to revoke a declaration of a SISTO by gazette notice to reflect the change in operation or in the wider threat environment. A declaration may be revoked if the chief executive reasonably believes that a surface transport operation is no longer at an 'elevated risk.' It sets out that this may occur due to the receipt of new intelligence or a change in the SISTO's circumstances.

Chapter 3 SISTOs

Part 1 Preparing risk management plan

Clause 15 requires that the SISTO must take all reasonable steps to prepare and implement a risk management plan as part of the regulatory regime as described under this part.

Sub-section (1) outlines that the preparation of a risk management plan must be completed so that a copy of the risk management plan is provided to the chief executive in written or electronic form within the time stated in the declaration notice. It prescribes the maximum penalty that can be imposed for a breach of this provision.

Sub-section (2) defines the term "prescribed period". If no time is stated, a copy of the risk management plan must be provided to the chief executive within three (3) months after the declaration notice is gazetted.

Clause 16 requires that a risk management plan for the SISTO must be prepared in accordance with the counter terrorism standard as prescribed under a regulation.

Sub-section (1) (b) provides that if the counter terrorism standard does not provide for a matter the AS/NZS 4360:2004 Australian standard can be used.

Sub-section (2) states the objectives of developing a risk management plan. These objectives provide the basis for developing a confident and rigorous basis for decision-making and planning. They are to prevent or reduce the risks of a terrorist act involving the SISTO; mitigate the effects of any terrorist attack; provide for recovery and continuity after any terrorist attack; and that SISTOs are required to communicate and cooperate if they are in proximity to other SISTOs as well as other owners and operators in the development of risk assessments and risk management plans.

Sub-section (3) specifies that the Bill recognises that SISTOs may have existing risk management plans in place. Provided that these documents address the threat and consequences of terrorism under an 'all hazards approach', the planning requirements may comprise an existing plan that complies with clause 17. An 'all hazards approach' includes preparing risk mitigation strategies for not only the threat or act of terrorism, but also natural and accidental disasters which may include flood, fire or theft as many measures may be similar.

Sub-section (4) defines the term "AS/NZS".

Clause 17 specifies the contents required of a risk management plan under the Bill.

Sub-section (1) requires the SISTOs risk management plan to provide detail to assess the risk of a terrorist act or security incident to the operation and the measures to be undertaken to prevent, or reduce those risks. The risk management plan should take into consideration the possibility of a change in the threat environment. This should include the level and type of risk present and be responsive to enable a pre-planned change in measures, to meet the change in the threat environment.

A risk management plan builds the processes necessary for increasing preparedness for uncertain circumstances, such as a security incident. Further, a systematic and critical examination demonstrates a commitment and provides the platform for preventative systems to be put in place. A risk management plan also fosters an active approach to mitigating risk to the surface transport operation and to the community.

A risk management plan may describe measures to mitigate risk to be implemented over a period of time. Interim measures, however, should meet those risks identified in the intervening period.

Sub-section (2) requires the risk management plan to specify immediate response procedures; the procedures for recovery; and the procedures for continuity of service of the SISTO to be taken in the event of a security incident.

It also provides for communicating with the Queensland Police Service; communicating with the chief executive, other related SISTOs and neighbouring facilities. Effective communication and consultation is essential to ensure that those responsible for implementing risk management, and those with a vested interest, understand the basis on which certain decisions are made and why particular actions are required.

The plan must be coordinated with other plans required by the *Dangerous Goods Safety Management Act 2001,* the *Disaster Management Act 2003*, and the potential exercise of power under the *Public Safety Preservation Act 1986*.

Sub-section (3) requires the risk management plan to state the training regime of SISTO employees and provide for a record of this training. Well-trained staff familiar with their local environment can contribute greatly towards the increased preparedness for security incidents, particularly through implementing security measures and by identifying, reacting and responding to suspicious or unusual activity. Further, the training regime should impart upon staff a realistic understanding of what to do.

Sub-section (4) requires the risk management plan to identify each person who has an obligation under the plan to be clearly identified by position and title.

Sub-section (5) requires the risk management plan to state emergency contact details and measures for maintaining the security of the plan. This provides a point of contact between government and industry to ensure the risk of terrorism is being mitigated and that the SISTOs obligations are being met under the Bill. The risk management plan and other auditable records should also be stored in an appropriate secure storage container with an appropriate classification, for example “security-in-confidence”.

Sub-section (6) states that if the SISTO has 1 or more related SISTOs, the risk management plans must include coordination arrangements between

the plans. This will typically involve a range of measures based on risk, coordinated during the development of the risk management plan. For example, maintaining a security dialogue between the SISTOs or sharing detailed emergency evacuation and procedure plans.

Sub-section (7) defines the term "relevant training".

Clause 18 allows the chief executive to provide guidelines for risk management plans however, if these guidelines are inconsistent with the documents in 16(1) then these documents prevail. These guidelines may include guidance on where specific areas of risk may be found but do not substitute for a risk assessment performed under AS/NZS 4360:2004 or the counter-terrorism standard.

Part 2 Other provisions about plan

Clause 19 requires the SISTO to implement the risk management plan as soon as possible after its development and ensure that each person who has an obligation under the plan complies with it.

A failure of a declared SISTO to implement the risk management plan signifies that the operation is putting the community at risk of the adverse impacts of terrorism. It prescribes the maximum penalty that can be imposed for a breach of this provision.

Clause 20 requires a SISTO to ensure the risk management plan is audited annually by the SISTO or an independent entity. It provides for the verification that the risk management plan is being implemented in accordance with its contents. A rigorous audit process ensures that the SISTOs obligations under the Bill of mitigating the risk of terrorism are met. Not undertaking an audit is equivalent to not having a valid risk management plan in place. It also prescribes the maximum penalty that can be imposed for a breach of this provision.

Clause 21 details the information that an audit carried out under clause 20 must state and that the record must be kept for 3 years. It prescribes the maximum penalty that can be imposed for a breach of this provision.

Clause 22 requires a SISTO to ensure that the risk management plan is reviewed at appropriate times to ensure its continued compliance with the Bill. Not reviewing the plan in light of a change of circumstances is

comparable to not having a compliant risk management plan. It prescribes the maximum penalty that can be imposed for a breach of this provision.

Sub-section (2) specifies the circumstances after which a review must occur. The review event may be after the receipt of an amended declaration; an audit or exercise identifying a systemic problem with the plan; a change in SISTO's circumstances affecting the SISTO's level of risk; a security incident involving the SISTO; or 5 years after the risk management plan was prepared or last reviewed.

Clause 23 details the information that a review carried out under clause 22 must state in the record and that the record must be kept for 3 years. It prescribes the maximum penalty that can be imposed for a breach of this provision.

Clause 24 provides for the SISTO entity to amend the risk management plan after a review.

Sub-section (1) requires that if the SISTO becomes aware of a deficiency in the risk management plan, the entity must rectify the deficiency within 28 days by implementing correctly, or by revising the plan in light of the audit or review. Not amending the plan is comparable to not having a valid and compliant risk management plan. It prescribes the maximum penalty that can be imposed for a breach of this provision.

Sub-section (2) requires that the SISTO must give a copy of the amendment, or a copy of the plan as amended, to the chief executive 28 days after the amendment was made. It prescribes the maximum penalty that can be imposed for a breach of this provision.

Sub-section (3) defines the term "deficiency" in terms of its relationship to the content of the plan.

Clause 25 requires the SISTO to prepare, conduct and participate in an exercise to test the operation of the SISTO's risk management plan, at least once a year. Exercising is integral to training, developing and preparing personnel to carry out functions in real emergencies.

An exercise may consist of either a desktop or operational exercise to test the risk management plan. In a situation where a desktop scenario is used as a basis to test the operation of the plan, the exercise should be sufficiently robust to test the actual adequacy of the plan under conditions of stress.

Sub-section (1) outlines that the SISTO may fulfil its obligations under the act by planning, conducting and participating in one or more exercises that

comply with the prescribed standard. The SISTO may also contribute and participate in an exercise conducted by another entity. The SISTO must take all reasonable steps to ensure that each person that has obligations under the plan participate in the exercises. The exercise need not test all parts of the risk management plan. The Bill recognises that exercises can be expensive enterprises and different parts of the plan may be tested over consecutive years. It prescribes the maximum penalty that can be imposed for a breach of this obligation.

Sub-sections (2) and (3) require the SISTO's entity to take all reasonable steps to comply with a direction from the chief executive to test the operation of the risk management plan through a multi-agency exercise. It prescribes the maximum penalty that can be imposed for a breach of this obligation.

Sub-section (4) requires the SISTO's entity to submit a copy of the plan for the exercise with the date and time of the exercise to the chief executive at least 28 days before conducting an exercise. It prescribes the maximum penalty that can be imposed for a breach of this obligation.

Sub-section (5) states that an authorised officer may observe the exercise.

Sub-section (6) defines the term “prescribed standard”.

Clause 26 requires the SISTO to keep a record of each exercise conducted under clause 25. The record must contain the date the exercise was conducted; the name and contact details of the person who planned and conducted the exercise; what part of the risk management plan was tested; and that the record must be kept for 3 years. It prescribes the maximum penalty that can be imposed for a breach of this obligation.

Clause 27 provides that each year a SISTO must provide the chief executive with an annual certificate. The annual certificate confirms that the SISTO is meeting its ongoing regulatory requirements under the Bill.

Sub-section (1) states that the SISTO must give the chief executive an annual certificate (in the approved form) which describes the auditing, reviewing and testing of the plan. It prescribes the maximum penalty that can be imposed for a breach of this provision.

Sub-section (2) provides that the annual certificate must be signed by, or for, the surface transport operation and be submitted to the chief executive before 1 September, or a date directed in writing by the chief executive.

Sub-section (3) specifies what the annual certificate must state to confirm ongoing compliance.

Clause 28 requires the SISTO to submit written notice of a change of emergency contact details within 2 business days after becoming aware of the change to the chief executive and related SISTOs. This maintains a point of contact between government and industry as well as related SISTOs. It prescribes the maximum penalty that can be imposed for a breach of this provision.

This provision should also provide the impetus for the SISTO to provide the change of contact details to the Queensland Police Service or emergency services in relation to the plan in the event of a security incident**.**

Chapter 4 Monitoring and enforcement

Part 1 Authorised officers

Clause 29 provides that the chief executive may appoint as an authorised officer an officer of the department, or another person decided by the chief executive, only if the chief executive is satisfied the person is qualified for the appointment, because the person has the necessary expertise or experience.

Clause 30 states the conditions under which an authorised officer holds office. It specifies that a signed notice given to the authorised officer, or a regulation, may limit the authorised officer's powers under the Bill.

Sub-section (3) defines the term "signed notice".

Clause 31 requires the chief executive to give each authorised officer an identity card.

Sub-section (2) describes the content of the identity card.

Sub-section (3) provides that this section does not prevent the issue of a single identity card for this Bill and other purposes.

Clause 32 states that an authorised officer must produce or display the identity card in exercising power under the Bill.

Sub-section (2) specifies that if it is not practicable to display the identity card in the first instance, the authorised officer must display the card at the first reasonable opportunity.

Sub-section (3) provides that an authorised officer does not exercise power only because an authorised officer has entered a place under clause 36(1)(b) or (3) which includes entering a public place or entering a place to ask consent.

Clause 33 states that an authorised officer ceases to hold office when the term of office ends; under another condition of office, the officer ceases to hold office; or under clause 34 the officer resigns. These do not limit the ways an authorised officer may cease office.

Sub-section (3) defines the term "condition of office".

Clause 34 states that an authorised officer may resign by a signed notice given to the chief executive.

Clause 35 requires a person ceasing to be an authorised officer to return the identity card to the chief executive within 7 days after ceasing to be an authorised officer, unless the person has a reasonable excuse. It also prescribes the maximum penalty that can be imposed for a breach of this obligation.

Part 2 Powers of authorised officers

Division 1 Entry of places

Clause 36 defines the conditions under which an authorised officer has power to enter places.

Clause 37 defines the procedures to be observed by an authorised officer seeking the consent of an occupier to enter a place.

Division 2 Entry of prescribed vehicles

Clause 38 defines the conditions under which an authorised officer has power to enter vehicles.

This power is necessary under the Bill, as operators that are declared SISTOs may keep their risk management plans and auditable documents secured within a vehicle, for example, ferries.

Clause 39 defines the procedures to be observed by an authorised officer seeking the entry of a vehicle.

Sub-section (5) defines the term "owner".

Division 3 General enforcement powers

Clause 40 applies to authorised officers that have entered a place or vehicle with consent.

Clause 41 defines the general powers that may be exercised by an authorised officer after entering a place or vehicle if consent is given or the entry is otherwise authorised to determine compliance under the Bill's regulatory regime.

Clause 42 requires a person to give reasonable assistance to an authorised officer in the exercise of the officer's powers, unless the person has a reasonable excuse. The officer may direct a person to provide assistance verbally, or in writing. This may include, but is not limited to: find and gain access to records or information; recording information in a useful form; or find and gain access to electronically stored information. It is a reasonable excuse not to comply with the requirement if it might tend to incriminate the individual. It also prescribes the maximum penalty that can be imposed for a breach of this obligation.

Sub-section (5) defines "relevant person".

Division 4 Other powers

Clause 43 provides an authorised officer with the power to require a person to state the person's name and residential or business address in specified circumstances. The requirement to provide a persons name and address allows authorized officers to identify those persons with a responsibility specified in a risk management plan under subsection 17 (5).

Clause 44 requires a person to provide name and address details, if required to do so by an authorised officer. It prescribes the maximum penalty that can be imposed for a breach of this obligation.

Clause 45 provides an authorised officer with the power to require information or to produce documents under specified circumstances from a person in investigating an offence against this Bill, unless the person has a reasonable excuse. The documents that may be employed to monitor compliance include:

- SISTO risk management plan;
- SISTO risk management implementation plan;
- SISTO audit register;
- SISTO risk management plan audit report;
- SISTO risk management plan review register;
- SISTO exercise records;
- SISTO emergency contact information register;
- SISTO training register;
- SISTO security and emergency equipment test register;
- Security procedures – listed in manuals, position descriptions, quick reference guides and pocket cards;
- Security awareness information – contained within organisational magazines, newsletters, brochures, notices;
- Security coordination meetings – including agendas, team meeting minutes, lists of representatives;
- Closed Circuit Television (CCTV) maintenance and monitoring records;

- Purchase orders, invoices, payment advice records relating to hiring security consultants, security guards, security monitoring, security and emergency equipment;
- Vehicle and person entry records including visitors registers and contractors registers;
- Electronic access control system records;
- Alarm system records;
- Security patrol rosters; and
- Security design documents – information relating to environmental design, building and surrounds maintenance.

It also prescribes the maximum penalty that can be imposed for a breach of this obligation.

Chapter 5 Powers of chief executive

Clause 46 provides the chief executive with power to give a SISTO a direction to comply with a prescribed provision in writing within a stated time, unless the controlling entity has a reasonable excuse. This provides the chief executive with a regulatory escalation power if a SISTO is not meeting its obligations under the Bill. It prescribes the maximum penalty that can be imposed for a breach of this provision.

Sub-section (3) defines the term "prescribed provision".

Clause 47 provides the chief executive with the power to seek a court order from the Supreme Court to suspend all or part of a SISTO if a SISTO presents an unacceptable risk of exposure to significant adverse impacts associated with a terrorist attack involving the SISTO. The chief executive would seek this remedy after repeated failures of a SISTO to fulfil its obligations under the Bill.

This provision is not intended to be used as a response to a change in the threat environment.

Sub-section (4) requires the chief executive to make application stating previous convictions, and the particulars of the alleged persistent failure to comply.

However, should an incident occur, or where a state of emergency is declared, the *Disaster Management Act 2003*, or the *Police Powers and Responsibilities Act 2000*, or the *Public Safety Preservation Act 1986* supersedes any arrangement under this Bill.

Sub-sections (5) and (6) allows the Supreme Court to make an order if it is satisfied that the SISTO entity has been convicted of an offence, and satisfied that the chief executive reasonably believes there is an unacceptable risk. The order may suspend all or part of the SISTO operation.

Chapter 6 Other enforcement matters

Clause 48 prohibits providing false or misleading statements to the chief executive or authorised officer and prescribes the maximum penalty for non-compliance.

Clause 49 prohibits providing false or misleading documents to the chief executive or authorised officer and prescribes the maximum penalty for non-compliance.

Sub-section (2) provides that for conditions for when this clause does not apply.

Clause 50 prohibits obstructing an authorised officer in the exercise of power under this Bill, without a reasonable excuse. It also prescribes the maximum penalty that can be imposed for a breach of this provision.

Sub-section (3) defines the term “obstruct”.

Clause 51 prohibits pretending to be an authorised officer and prescribes the maximum penalty for non-compliance.

Chapter 7 Legal proceedings

Part 1 General

Clause 52 describes the proceedings for offences and that offences under this Bill are summary.

Clause 53 requires the Court to make orders it considers appropriate for publication of proceedings and whether to allow those proceedings to be heard in closed court. A closed court may be necessary to ensure limited communication of confidential material produced by government agencies or the SISTO.

Clause 54 provides for the protection of counter-terrorism information during legal proceedings. In a proceeding before a court or tribunal, the court or tribunal may excuse a person from the requirement to disclose information, if disclosure is likely to prejudice the prevention, investigation or prosecution of a terrorist act or suspected terrorist act; disclosure is likely to prejudice national security; under the *National Security Information (Criminal and Civil Proceedings) Act 2004 (Cwlth)* and the *Police Powers and Responsibilities Act 2000*, section 803, a police officer would not be required to disclose information; or if it was in the public interest in preserving secrecy.

Part 2 Other provisions about proceedings

Clause 55 provides that the executive officers of a surface transport operation must ensure that the SISTO complies with obligations under this Bill.

Sub-section (5) defines the term "executive officer".

Clause 56 states that an entity may avoid liability if the entity can demonstrate they took all reasonable steps in relation to the matter to comply with the obligations of the Bill.

Chapter 8 Miscellaneous

Clause 57 provides that a person must not disclose, record or use information the person gained through involvement in the administration of the Bill, or because of the opportunity provided by the involvement. This allows for limited communication of confidential material. It prescribes the maximum penalty that can be imposed for a breach of this provision.

Sub-section (2) provides the circumstances under which information may be disclosed, recorded or used under the Bill.

Sub-section (3) defines the term "disclose".

Clause 58 provides for the protection of civil liability of an official.

Sub-section (3) defines the term "official".

Clause 59 provides that the chief executive may approve forms for use under this Bill.

Clause 60 provides for the making of regulations by the Governor in Council. A regulation may prescribe offences for a contravention of a regulation and fix a maximum penalty of no greater than 20 penalty units.

Clause 61 provides for a review of the Act after five years from the commencement date. The Minister must table a report of the review's outcomes in the Legislative Assembly within twelve months following the end of the five year period.

Schedule

Dictionary

Defines the meaning of particular words used in this Bill.