

# Terrorism (Community Protection) Bill

## Circulation Print

### EXPLANATORY MEMORANDUM

#### General

The Bill provides new powers and obligations to assist in preventing, or responding to, potential terrorist acts.

#### Clause Notes

##### PART 1—PRELIMINARY

- Clause 1 sets out the main purposes of the Bill, which are—
- to provide new powers and obligations in relation to the prevention of, and response to, terrorist acts;
  - to provide for a covert search warrant regime;
  - to provide for mandatory reporting of the theft or loss of certain chemicals and substances;
  - to impose risk management obligations on operators of certain essential services; and
  - to protect counter-terrorism methods from disclosure in legal proceedings.
- Clause 2 provides for the commencement of this Bill. Parts 1 (preliminary), 3 (police powers to detain and decontaminate), 5 (protection of counter-terrorism information), 7 (general) and 8 (amendment to **Freedom of Information Act 1982**, etc) commence on the day after the day on which the Bill receives Royal Assent. The remaining provisions commence on a day or days to be proclaimed, in order to allow regulations to be made and other administrative steps to be taken. If any provision of the Bill has not come into operation before 1 July 2004, then it will come into operation on that date.

Clause 3 sets out the definitions used in the Bill. These include the key definitions of "counter-terrorism information", "essential service" (which is defined in more detail in clause 26) and "operator". "Terrorist act" is defined separately in clause 4.

Clause 4 sets out the definition of a "terrorist act". This definition is in the same terms as that in Chapter 5, Part 5.3 of the Commonwealth Criminal Code.

## **PART 2—COVERT SEARCH WARRANTS**

Clause 5 provides that a warrant for a covert search may only be issued by a judge of the Supreme Court.

Clause 6 sets out the grounds on which a member of the police force can apply to the Supreme Court for a covert search warrant. A member of the police force can only apply for a covert search warrant with the approval of the Chief Commissioner of Police, a Deputy Commissioner or an Assistant Commissioner.

In addition, the member of the police force who makes the application must suspect or believe, on reasonable grounds, that—

- a terrorist act (as defined in clause 4) has been, is being or is likely to be committed; and
- entering and searching the premises would substantially assist in preventing or responding to the terrorist act or suspected terrorist act; and
- it is necessary to enter and search the premises without the knowledge of the occupier of the premises.

Ordinarily members of the public may attend legal proceedings, and the media may report the proceedings. Clause 6(2) requires the court to be closed to the public whenever it hears an application for a covert search warrant. This is to ensure that information that could jeopardise the successful conduct of the search is not made public.

Clause 7 sets out how an application for a covert search warrant should be made. An application must be in writing, supported by an affidavit. It must state the grounds on which the warrant is sought. The court must not issue the warrant unless the grounds on which the warrant is being sought are included on the application, and the applicant provides the court with any further information the court requires on why the warrant is being sought.

Clause 8 sets out the criteria the court must consider in deciding whether to issue a covert search warrant. The court must be satisfied that there are reasonable grounds for the suspicion or belief that the warrant is necessary. It must also consider—

- the nature and gravity of the terrorist act or suspected terrorist act; and
- the extent to which the exercise of powers under the warrant would assist the prevention or response to a terrorist act or suspected terrorist act; and
- the extent to which any person's privacy would be affected.

Clause 8(2)(d) provides the court with a discretion to impose any other conditions on the warrant that it considers necessary and appropriate in the circumstances. For example, the reason why the search has to be covert may be temporary. If the reasons for the covert search will be short-lived, the court could impose a condition that the police notify the occupier of the searched premises after a certain period. This provides an additional safeguard on the issuing of a covert search warrant and is intended to ensure that the covert search warrant power is not abused.

Clause 8(3) sets out the details that must be specified in the warrant. These are—

- that the purpose of the warrant is to assist the prevention of, or response to, a terrorist act or suspected terrorist act; and
- the address or location of the premises to be searched; and
- the name of the member of the police force who is applying for the warrant; and
- the name or identity of the persons who may enter and search the premises; and
- whether more than one entry is authorised; and
- the date on which the warrant is issued; and
- the duration of the warrant (which cannot exceed 30 days); and

- the names of any occupiers of the premises to be searched (if known); and
- the name or description of the kind of thing to be searched for, seized, placed, copied, photographed, recorded, operated, printed, tested or sampled; and
- any further conditions.

Clause 9 sets out the things a covert search warrant allows a member of the police force to do. The person named in the warrant can enter the premises by force (using any necessary equipment) or by impersonation. The premises must be those specified in the warrant, or other specified premises which adjoin or provide access to the premises described in the warrant.

Clause 9(1)(a)–(g) sets out the range of activities which a covert search warrant allows.

Clause 9(2) allows the Supreme Court to direct that anything seized under a warrant be returned to its owner, if in the opinion of the Court it can be returned consistently with the interests of justice. The Court may impose any conditions it considers necessary upon the return of any such items.

Clause 10 allows an application to be made by telephone where a covert search warrant is needed urgently. In urgent circumstances, a member of the police force must first prepare an affidavit setting out the grounds on which the warrant is sought. If necessary, however, the member may make the application before the affidavit is sworn.

Clause 10(3) provides that if a fax machine is available, the member must fax a copy of the affidavit to the Supreme Court.

The Supreme Court may issue a warrant on application by telephone after—

- considering the terms of the affidavit; and
- receiving any further information that may be required concerning the grounds on which the warrant is being sought; and
- being satisfied as required by clauses 7(2) and 8(1); and
- having regard to the factors in clause 8(2).

Clause 10(5) provides that if the Supreme Court issues a covert search warrant by telephone, it must inform the applicant of the terms of the warrant (the list of which is set out in clause 8(3)), the date it was issued and record the reasons it was issued on the warrant. If possible, a copy of the warrant must be faxed to the applicant.

Clause 10(6) provides that if a copy of the warrant has not been faxed to the applicant, the applicant must complete a form of warrant in the terms communicated to the applicant by the Supreme Court and must write the name of the judge who granted the warrant and the date and time of issuing.

The applicant must then send the form of warrant to the Court not later than the day after the execution of the warrant or the expiry date of the warrant, whichever is earlier.

Clause 10(7) provides that if an application for a covert search warrant is made by telephone, the applicant must send the original sworn affidavit to the Supreme Court no later than the day after the application. This affidavit must be sent to the Court whether or not the warrant is issued.

Clause 10(8) provides that where it is material for a court to be satisfied that an entry, search or seizure was authorised in accordance with clause 10 and a covert search warrant is not produced in evidence, the court must assume (unless it is proved otherwise) that the entry, search or seizure was not authorised by such a warrant.

Clause 11 sets out additional safeguards. The person to whom the warrant is issued must make a report to the Supreme Court no later than 7 days after the warrant expires. Failure to make a report carries a maximum penalty of 1 year imprisonment or a fine of 120 penalty units (currently \$12 000) or both.

Clause 11(2) sets out the matters which must be contained in the report.

Clause 12 prohibits the publishing of any report of the whole or part of a proceeding for an application for a warrant, or any information derived from such a proceeding or part of any report made to the Supreme Court, unless the Court orders otherwise. The maximum penalty is 2 years jail in the case of a natural person or a fine of 240 penalty units (currently \$24 000) or both, and in the case of a corporation, 1000 penalty units (currently \$100 000) for a first offence and 20 000 penalty units (currently \$2 000 000) for a subsequent offence.

Clause 13 provides that the Chief Commissioner must submit an annual report on covert search warrants to the Minister. The report must contain the information listed in clause 13(1)(a)–(h). The Minister must table the report before both Houses of Parliament within 12 sitting days of receiving the report.

### **PART 3—POLICE POWERS TO DETAIN AND DECONTAMINATE**

Part 3 provides members of the police force with new powers to detain and to authorise the decontamination of people who have been (or may have been) exposed to contamination from chemical, biological or radiological agents as part of a terrorist act.

The Bill sets out the process for granting an authorisation to use these powers and describes the powers that are available under this Part.

Clause 14 expresses the Parliament's intention that an authorised member of the force when exercising the powers under this Part must do so without imposing unnecessary limitations on personal liberties and privacy. For example, where practicable, persons detained have a right to communicate by phone with family or friends, to have their privacy protected and to receive information about the medical consequences of disease or contamination and the appropriate treatment.

Clause 15 sets out the definitions used in Part 3, including the key definition of "danger area". "DISPLAN" and "emergency" are defined as having the same meaning as in the **Emergency Management Act 1986**.

"DISPLAN" is the State emergency response plan prepared under section 10 of that Act.

"Emergency" is exhaustively defined in section 4(1) of that Act. The definition includes events such as—

- an explosion;
- a plague or an epidemic;
- a warlike act, whether directed at Victoria or a part of Victoria or at any other State or Territory of the Commonwealth;
- a hi-jack, siege or riot; and
- a disruption to an essential service.

- Clause 16 empowers a senior police officer of the rank of inspector or above to give an authorisation only when that officer has a reasonable belief that a terrorist act has or may have occurred and that as a result of that act an area or persons in that area may have been exposed to contamination.
- Clause 17 sets out the authorisation process. An authorisation may be given orally or in writing. If an authorisation is given orally, it must be confirmed in writing. The authorisation must specify that it is given under this Part, describe the terrorist act or suspected terrorist act, name the member of the force to whom the authorisation is given, the time the authorisation is given and the area or persons that may have been exposed to contamination.
- Clause 18 describes the police powers authorised under this Part. A member of the force may (or may direct another member of the force to, in respect of a person in the danger area)—
- direct persons to enter, not enter or to leave a premises or area;
  - detain a person or persons; and
  - require a person to submit to decontamination.

This clause also establishes a power for an authorised member of the force to authorise an officer, employee or volunteer of an emergency services agency to undertake decontamination of persons exposed to contamination by a terrorist act. Submitting to decontamination can include processes such as being sprayed with water or chemical decontaminants.

Clause 18(2) deals with oral directions. It provides that, if an oral direction is made to a group of people, it is deemed to have been given to each member of the group if it has been made in a manner that is likely to be audible to all members of the group or as many of them as is reasonably practicable.

Clause 18(3) provides an ancillary power enabling an authorised member of the force to give any direction necessary to effectively exercise the powers in clause 18(1). For example, this might include a direction that exposed persons be moved to another site for decontamination.

Clause 18(4) requires the police to facilitate any reasonable request by a person detained under clause 18(1)(c) to communicate with a person such as a friend, relative, lawyer or doctor. Whether a particular request is reasonable will depend on the circumstances (such as the extent to which access to means of communication such as telephones can be provided to victims

consistently with the objective of limiting the spread of contamination).

Clause 19 provides that an authorisation will lapse if—

- the senior police officer who gave the authorisation under clause 16 notifies the Chief Commissioner that he or she no longer believes that a terrorist act has or may have occurred and that an area or people may have been exposed to chemical, biological or radiological contamination;
- the agency primarily responsible under DISPLAN has taken responsibility for responding to the contamination and has advised the Chief Commissioner that the authorisation should lapse; or
- eight hours have passed since the giving of the authorisation (unless the authorisation has been extended under clause 20).

"DISPLAN" was originally the short title for the State Disaster Plan. Amendments to the **Emergency Management Act 1986** in 1994 replaced the term "disaster" with "emergency". The term "emergency response" has now replaced the term DISPLAN in official usage and the State Emergency Response Plan set out in the Emergency Management Manual Victoria is the document which fulfils the functions of DISPLAN as required by the Act.

The Emergency Management Manual Victoria (issued under the **Emergency Management Act 1986**) sets out the agreed administrative protocols for all agencies when responding to an emergency. These police powers are to be used in a way that is consistent with the state emergency plans.

Clause 20 provides that in limited circumstances the authorisation may be extended beyond eight hours. An extension must be authorised by the Chief Commissioner, a Deputy Chief Commissioner or an Assistant Commissioner and an extension can only be granted with the agreement of the relevant government agency responsible for responding to the contamination.

Clause 21 enables a member of the police force to use reasonable and necessary force if a person refuses to comply with a direction given under this Part.

#### **PART 4—MANDATORY REPORTING OF THEFT OR LOSS OF PRESCRIBED CHEMICALS AND OTHER SUBSTANCES**

Clause 22 provides for mandatory reporting of the theft or loss of prescribed chemicals or substances. The obligation will be on the occupier of the premises from where the chemical or substance was stolen or lost. The definition of "premises" in clause 3 includes a vehicle. Therefore, the reporting obligations would apply, for example, to the loss of chemicals from a truck in which they were being transported.

On becoming aware of a theft or loss, the occupier must notify police without delay, and may be required by police to provide a written report.

Failure to inform the police, or to make a written report if requested, carries a maximum penalty of 10 penalty units (currently \$1000) in the case of a natural person, and 120 penalty units (currently \$12 000) in the case of a corporation.

This provision is intended to provide police with information which may help prevent a terrorist act by alerting police to the disappearance of chemicals such as those used in the October 2002 Bali bombing.

The specific chemicals and substances, and threshold amounts to which the reporting obligation relates will be prescribed by regulation.

#### **PART 5—PROTECTION OF COUNTER-TERRORISM INFORMATION**

Clause 23 provides that in certain circumstances counter-terrorism information may be protected from disclosure in legal proceedings. "Counter-terrorism information" is defined in clause 3 as information which relates to covert methods of investigation into a terrorist act, or suspected terrorist act. This information may be protected where disclosure of it would prejudice the prevention, investigation or prosecution of a terrorist act (or suspected terrorist act) and the public interest in protecting the information outweighs the public interest in disclosure.

Where a person would otherwise be required to disclose counter-terrorism information, and protection under Part 5 is appropriate, the person will be excused from the requirement to disclose that information. The definition of "legal proceeding" is drawn from the **Evidence Act 1958** and includes any civil or criminal proceeding before a court, a coronial inquest, and a royal

commission. The protection is available at any stage of a legal proceeding, and applies to any disclosure of information, not just the formal adducing of evidence.

The protection of counter-terrorism information is not a blanket protection. Where information falls within the definition of counter-terrorism information and its disclosure may prejudice prevention, investigation or prosecution of a terrorist act, a case by case decision must be made about whether the public interest in protecting the information (for example, the interest in effective investigation of terrorist activity which relies on the protection of covert methods) is greater than the public interest in disclosing the information (for example, in a criminal proceeding, the interests of justice served by the defendant having access to all relevant information to defend the case). The same balancing exercise is currently required at common law, under the doctrine of public interest immunity.

The decision about the potential impact of disclosure and where the balance between public interests lies will be made by a court. In making this decision, the court must consider the matters listed in clause 23(2). The court is not limited to consideration of only the matters listed in clause 23(2). Clause 23(3) provides that in making a decision under clause 23, the court may inform itself in any way it thinks fit.

Clause 24 provides that, in making a decision under clause 23, the court may inspect a document for which protection is being considered. In some cases, though not all, inspection may be necessary in order to properly assess the weight of the public interest in protecting information.

## **PART 6—ESSENTIAL SERVICES INFRASTRUCTURE RISK MANAGEMENT**

Clause 25 sets out the object of Part 6, which is to provide for operators of essential services to be involved in planning the protection of those essential services against terrorist acts.

Clause 26 sets out the definition of "essential service".

Clause 27 sets out the definition of "relevant Minister".

Clause 28 provides that the Governor in Council may declare any particular essential service, or any part of an essential service, to be a "declared essential service". Part 6 will only apply to an essential service, or part of an essential service, which has been declared under clause 28. Clause 28(2) provides examples of what may constitute "part" of an essential service.

Clause 28(3) provides that the Governor in Council may specify that a person, or a person in a specified class of person, is the "operator" of a declared essential service. The definition of "operator" in clause 3 provides that if no person or class of persons is specified by the Governor in Council, then the "operator" is the person with day-to-day management of the declared essential service.

- Clause 29 provides that the operator of a declared essential service must prepare a risk management plan for the essential service. This must be done within the time determined by the relevant Minister and notified to the operator. The risk management plan required by Part 6 may form part of any other broader risk management plan prepared by the operator for the essential service.
- Clause 30 sets out the objectives of a risk management plan, which relate to preventing and responding to a terrorist act.
- Clause 31 sets out the requirements as to what a risk management plan must contain.
- Clause 32 provides that the operator of a declared essential service must ensure that the risk management plan, once prepared, is audited annually to ensure that it continues to meet the requirements in clause 31. The operator must address any deficiencies which are identified in the audit by amending the risk management plan. This must be done as soon as practicable after the audit.
- Clause 33 provides that an operator of a declared essential service must prepare and participate in a training exercise at least once a year (or less frequently, as determined by the Minister). The purpose of the training exercise is to test the risk management plan. The training exercise will be carried out under the supervision of the Chief Commissioner.
- The relevant Minister, in consultation with the Chief Commissioner and the operator, will determine the time and place of the training exercise.
- Clause 34 provides that the operator of a declared essential service must, if required to do so by the relevant Minister, certify in writing to the Minister as to whether or not a risk management plan has been prepared and/or audited in accordance with Part 6.
- Clause 35 provides that the operator of a declared essential service must, if required to do so by the relevant Minister, provide the relevant Minister with a copy of its risk management plan.

- Clause 36 provides that the relevant Minister may give a written direction to an operator to comply with the requirements to prepare a risk management plan (clause 29), to audit a risk management plan (clause 32), to participate in training exercises (clause 33), to certify compliance (clause 34), or to provide a copy of the plan (clause 35). The Minister may do this if he or she believes on reasonable grounds that the operator has failed to comply with one or more of these requirements. The Minister's direction will specify a time for compliance.
- Clause 37 provides that if an operator fails to comply with a direction from the relevant Minister (given under clause 36), the Minister may apply to the Supreme Court for an order requiring the operator to comply. Before making an order, the court must be satisfied that the operator has failed to comply with a direction from the Minister (under clause 36) within the time specified in the Minister's direction.

An application under clause 37 may involve disclosure of sensitive information about the operation of an essential service or about assessments of terrorist threats. It may therefore be appropriate for the application to be heard in closed court. This is a matter of discretion for the court, which has the power under section 18 of the **Supreme Court Act 1986** to close the court, to restrict who may be present in the court, or to restrict publication of proceedings, if to do so is necessary to protect the national or international security of Australia, or the physical safety of any person.

#### **PART 7—GENERAL**

- Clause 38 provides that the operation of the Act must be reviewed by 30 June 2006. The Bill is introduced to deal with the current increased terrorist threat. It is important that the powers and obligations contained in the Bill remain appropriate. Therefore, it is necessary for the Bill to be reviewed. This requirement to review is complemented by clause 41, which provides for automatic expiry of the Bill on 1 December 2006.
- Clause 39 provides that the Bill does not limit the operation of any other law. For example, the covert search warrant provisions in Part 2 of the Bill do not limit the **Surveillance Devices Act 1999**. If police want to place a listening device in premises, they must obtain a warrant to do so under that Act, rather than a covert search warrant under this Bill.
- Clause 40 provides regulation-making powers for the Bill.

Clause 41 is a sunset clause. It provides that the Bill expires on 1 December 2006. If legislation continues to be required to address terrorist threats, Parliament must pass appropriate legislation at that time.

### **PART 8—AMENDMENT TO FREEDOM OF INFORMATION ACT 1982 AND VICTORIAN CIVIL AND ADMINISTRATIVE TRIBUNAL ACT 1998**

Clause 42 inserts a new section 29A in the **Freedom of Information Act 1982**.

Section 29A provides a new exemption from the requirement to release documents which applies to documents affecting national security, defence or international relations. Under new section 29A, a document is an exempt document if its disclosure (under the **Freedom of Information Act 1982**) would, or could reasonably be expected to, cause damage to—

- the security of the Commonwealth or any State or Territory;
- the defence of the Commonwealth; or
- the international relations of the Commonwealth.

Under new section 29A(2), a Department Head or the Chief Commissioner may certify that a document requested would, if it existed, be an exempt document because it may affect national security, defence or international relations. Such a certificate establishes that the document is an exempt document.

The decision to give a certificate under new section 29A(2) cannot be investigated by the Ombudsman.

New section 29A will apply to a document whether it is created before or after the commencement of clause 42 of the Bill. Clause 2 of the Bill provides that clause 42 (which is within Part 8) commences on the day after the day on which the Act receives Royal Assent.

Clause 43 inserts a new section 53AA in the **Freedom of Information Act 1982**.

New section 53AA sets out the procedure where the Victorian Civil and Administrative Tribunal ("the Tribunal") determines that there are no reasonable grounds for the claim under new section 29A, being the claim made by a Minister giving a certificate. If the Tribunal makes such a determination, it must notify the responsible Minister. The responsible Minister must

then decide, within 28 days, whether or not to revoke the certificate given under new section 29A.

If the decision to issue the certificate is revoked, any claim made in the certificate is taken to be withdrawn and the Minister must inform the applicant of the existence, or non-existence, of the document to which the certificate related.

If the Minister decides not to revoke the decision to issue the certificate, he or she must notify the applicant and table a copy of the notice to the applicant in Parliament. The notice to the applicant must state the Minister's findings on any material question of fact, the material on which those findings are based and the reasons for the Minister's decision. It must also contain a copy of the Tribunal's notification to the Minister under new section 53AA(1). The notice to the applicant is not required to include any matter or information which would found a claim for an exemption (under section 28, 29A, 31(3) or 33) if that matter or information were in a document of an agency.

- Clause 44 makes consequential amendments to the **Freedom of Information Act 1982**. The most significant is new section 50(5A), which provides that the Tribunal does not have power to review a Minister's decision to certify that a document is exempt under new section 29A, but that the Tribunal may determine whether or not there are reasonable grounds for the claim that the document is an exempt document.
- Clause 45 inserts new clauses 29B, 29C and 29D in Part 8 of Schedule 1 to the **Victorian Civil and Administrative Tribunal Act 1998** to provide for the procedure of the Tribunal in reviewing a decision refusing to grant access to a document which is certified to be exempt under new section 29A of the **Freedom of Information Act 1982**. Under new section 50(5A) of the **Freedom of Information Act 1982**, the Tribunal does not have power to review a Minister's decision to certify that a document is exempt. However, under new clause 29B, the Tribunal shall, if requested by the applicant, determine whether there are reasonable grounds for the claim, by way of the Minister's certificate, for exemption under section 29A. For the purposes of making such a determination, the Tribunal must be constituted by a judicial member or judicial members.
- New clause 29D sets out requirements for holding certain parts of the proceeding in private. Any part of the proceeding during which evidence or information is given, or a document is produced, by an agency, a Department Head or the Chief Commissioner is to be heard in private. Also, any part of the proceeding during which a submission is made on behalf of an

agency, a Department Head or the Chief Commissioner in relation to the claim for exemption is to be heard in private. In relation to the part of the proceeding heard in private, the Tribunal may decide who may be present. Also, the Tribunal must give directions prohibiting publication of any evidence, information, documents or submissions given during any part of the proceeding which is held in private.