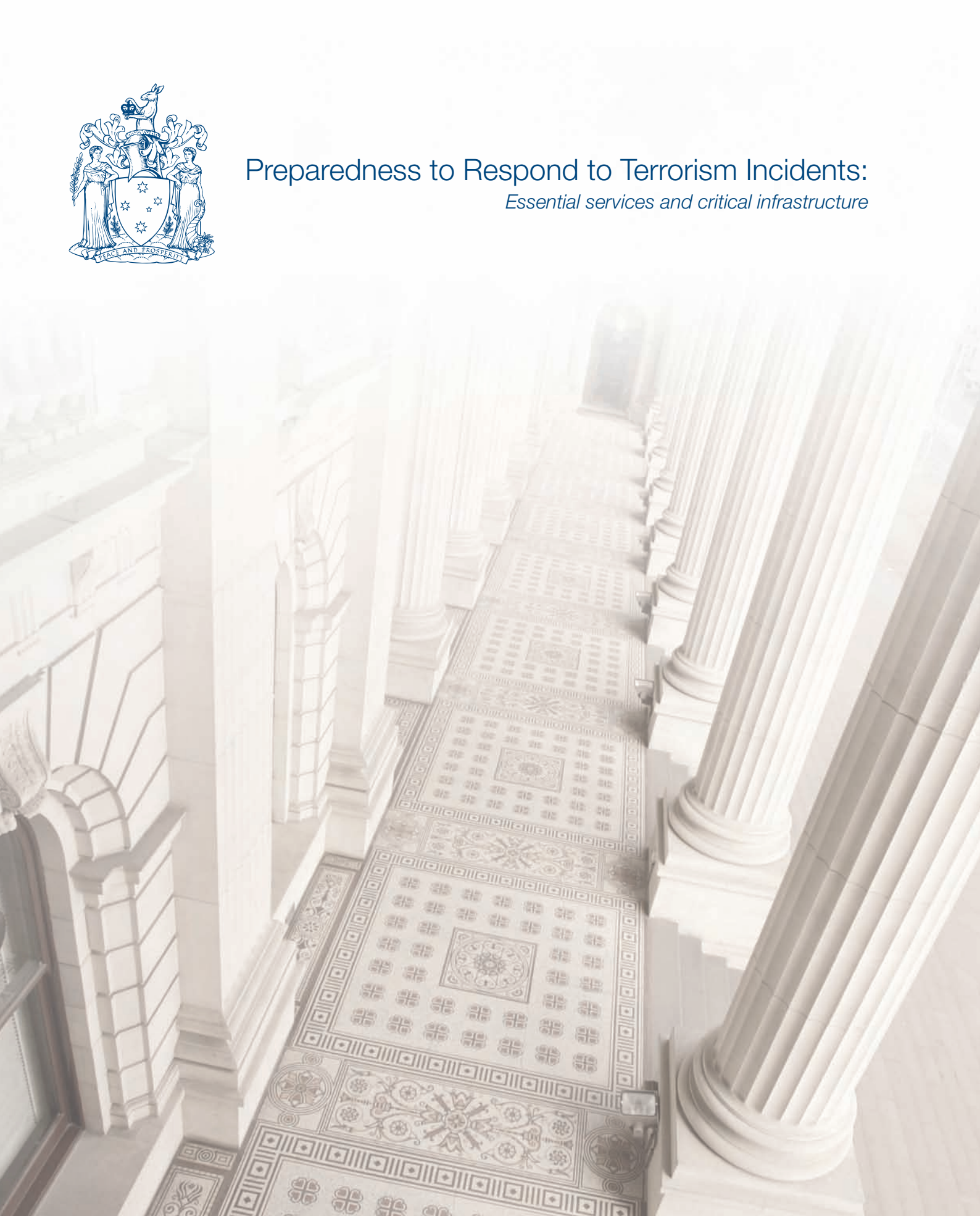
Preparedness to Respond to Terrorism Incidents:

Essential services and critical infrastructure



Victorian Auditor-General's Report | January 2009 | 2008-09:15

VICTORIA

Victorian
Auditor-General

Preparedness to Respond to Terrorism Incidents: *Essential services and critical infrastructure*

Ordered to be printed

VICTORIAN
GOVERNMENT PRINTER
January 2009

PP No 168, Session 2006-09

ISBN 1 921060 93 X

VAGO

Victorian Auditor-General's Office

Auditing in the Public Interest

The Hon. Robert Smith MLC
President
Legislative Council
Parliament House
Melbourne

The Hon. Jenny Lindell MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit my performance report on *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure.*

Yours faithfully

D D R PEARSON
Auditor-General

21 January 2009

Foreword

The right to live safely in an open, democratic and multicultural society is central to our Australian way of life. The devastating terrorist attacks on the United States in September 2001 struck at the heart of this core value, and galvanised governments across the world into acting to mitigate potential threats to their territories and people, from those determined to unsettle or destroy them.

In this more dangerous global security environment, which the recent attacks in Mumbai underscore, Victoria works in a cooperative partnership between national, state and territory jurisdictions, to implement the national counter-terrorism plan coordinated by the National Counter-Terrorism Committee.

Since 2002 Victoria has provided $255 million for state counter-terrorism initiatives, and has been an important and early contributor to developing the current national and state-level arrangements.

The government sector does not own and operate all of the services and infrastructure deemed to be essential or critical in Victoria. It has a clear interest, though, in preparing essential services and critical infrastructure to respond to many kinds of risk, including terrorist attack.

It is reasonable for citizens to ask how effective these preparations have been.

This audit of the arrangements to assist owners and operators of essential services and critical infrastructure has found that the arrangements are not as good as they could be. Some industry sectors are better than others. Some arrangements need to be clarified.

Stronger leadership is needed from the Department of Premier and Cabinet to administer legislation and supervise the arrangements. The department, to its credit, has commenced re-assessing the current arrangements.

D D R PEARSON
Auditor-General

21 January 2009

Contents

Acronyms

Acronym	Definition
CIP framework	Victorian Framework for Critical Infrastructure Protection from Terrorism
CIPU	Critical Infrastructure Protection Unit, Victoria Police
CGRC	Central Government Response Committee
DHS	Department of Human Services
DIIRD	Department of Innovation, Industry and Regional Development
DOJ	Department of Justice
DPC	Department of Premier and Cabinet
DPCD	Department of Planning and Community Development
DPI	Department of Primary Industries
DSE	Department of Sustainability and Environment
DOT	Department of Transport
IAAG	Infrastructure Assurance Advisory Group
SCN	Security and Continuity Network
G-SCN-CG	Government Security and Continuity Network Coordination Group
National CIP framework	National Guidelines for Protecting Critical Infrastructure from Terrorism
NCTC	National Counter-Terrorism Committee
SECC	Security and Emergencies Committee of Cabinet
SEU	Security and Emergencies Unit, Department of Premier and Cabinet
The Act	Terrorism (Community Protection) Act 2003

1 Executive summary

1.1 Introduction

The terrorist attacks in the United States in 2001 introduced a new and confronting dimension to the international security environment. Later attacks in Bali, Madrid, Jakarta and London confirmed that the terrorism threat is not limited to the United States. While Australia has not been directly attacked by terrorists, in recent times, its citizens and interests have been attacked offshore.

Since 2001, Australia's national counter-terrorism alert has been at the 'medium' level, meaning a terrorist attack within Australia could occur.

The 11 September 2001 terrorist attacks and the subsequent October 2002 Bali bombings prompted reform and enhancement of the national and Victorian counter-terrorism arrangements, through the introduction of new arrangements and legislation and the improvement of counter-terrorism capabilities.

Australia's counter-terrorism capability operates through a cooperative partnership between national, state and territory jurisdictions, with joint responsibility for developing and maintaining nationwide capability. The Commonwealth has the national coordination responsibility. The formation of the National Counter-Terrorism Committee (NCTC) in 2002 has driven the development of an approach to prepare for, respond to, and recover from potential terrorist attacks. Commonwealth, state and territory representatives make up the NCTC, which, among other things, is responsible for maintaining the national counter-terrorism plan. The plan sets out Australia's high-level strategy to prevent, and deal with acts of terrorism in Australia and its territories. It addresses capability, prevention, preparedness, response and recovery, and policy development, coordination and strategic arrangements.

1.1.1 Background

In November 2002 the Victorian government released its counter-terrorism policy statement *Enhancing Victoria's Domestic Security: New measures for the fight against terrorism*. The policy statement included requirements for Victoria Police to assist operators of essential services relating to electricity, gas, water, transport and fuel, in the development, validation and audit of their risk management plans and the coordination of joint exercises.

In 2003 the *Terrorism (Commonwealth Powers) Act 2003* and the *Terrorism (Community Protection) Act 2003* were introduced, establishing new counter-terrorism powers, including provisions for the protection of declared essential services. Victoria was the only jurisdiction to introduce essential services protection legislation. Later policy responses included *Protecting our Community: Attacking the Causes of Terrorism* released in September 2005 and *A Safer Victoria—Protecting our Community: New Initiatives to Combat Terrorism* in October 2006.

1.1.2 Essential services and critical infrastructure

Protecting essential services and critical infrastructure, is integral to minimising the impact and consequence of a terrorist attack. In June 2004 the Council of Australian Governments endorsed the NCTC's *National Guidelines for Protecting Critical Infrastructure from Terrorism* (the national CIP framework) as part of the broader national counter-terrorism arrangements. Victoria was an early starter in developing an approach to critical infrastructure protection and a significant contributor to and early proponent of the development of the national CIP framework.

Victoria's approach to critical infrastructure protection was influenced by the government's response to the Longford gas crisis of 1998 and by the fact that much of the state's essential services and critical infrastructure is privately owned or operated. Primary responsibility for providing adequate protection rests with owners/operators.

In April 2007 the government introduced the *Victorian Framework for Critical Infrastructure Protection from Terrorism* (the CIP framework), which draws on the national CIP framework, other nationally agreed documents for critical infrastructure protection, and is consistent with the national CIP framework. Among other things, the CIP framework formalised the involvement of Victoria Police in the validation and audit of risk management plans and the coordination of joint exercises for critical infrastructure.

Part 6 of the *Terrorism (Community Protection) Act 2003* (the Act) and the CIP framework together provide for the protection of essential services and critical infrastructure to enable continuity, or quick recovery of, service delivery and operations in the event of a terrorism incident.

The Act and the CIP framework operate within Victoria's emergency management arrangements, which are based on a common set of arrangements for all emergencies known as the 'all hazards, all agencies' approach. Under this approach all emergencies, regardless of their cause, are managed through arrangements set out in the *Emergency Management Act 1986*, the *Emergency Management Manual Victoria* and the *State Emergency Response Plan*. This means that the same agencies and arrangements used to respond to routine incidents and emergencies are also used to respond to terrorism incidents.

1.2 Audit objective and scope

The objective of this audit was to examine the state's preparedness to respond to terrorism incidents, relating to essential services and critical infrastructure.

In scope

The audit examined the governance arrangements established to assist operators of essential services and owners/operators of critical infrastructure to respond to terrorism incidents. The activities of selected Victorian government agencies with roles and responsibilities under Part 6 of the Act and the CIP framework were examined, including how they consulted and interacted with owners/operators of critical infrastructure and operators of declared essential services.

Specifically, we examined whether:

- governance aspects of the related state agencies—including roles, responsibilities and accountabilities—were clearly defined and understood
- inter-agency risks were identified and managed
- meaningful consultation and communication across government agencies and bodies and owner/operators occurred
- adequate performance monitoring occurred to assess progress with the implementation of Part 6 of the Act and the CIP framework
- the agencies audited had arrangements for monitoring the preparedness and capability of operators of declared essential services and owners/operators of critical infrastructure to respond to terrorism incidents.

The audit also considered funding for counter-terrorism initiatives including for preventing, responding to and recovering from terrorist attacks.

The activities of Victoria Police and seven Victorian government departments were examined.

Out of scope

Because of the focus of the audit on response, it did not examine:

- prevention activities involving collecting, analysing and disseminating intelligence about terrorist intentions and capabilities
- the implementation of additional powers to police, mandatory reporting of theft or loss of specified chemicals and substances, or the protection of counter-terrorism information introduced in the Act.

Regardless of the cause of an emergency, the response and recovery efforts of Victorian public sector agencies are set out under the state's 'all hazards, all agencies' approach to emergency management established by the *Emergency Management Act 1986*, the *Emergency Management Manual Victoria* and the State Emergency Response Plan. This means that the same agencies and arrangements used to respond to routine incidents and emergencies are also used to respond to terrorism incidents.

Given the audit scope, the audit did not examine the state's broader emergency management arrangements. Nor did it consider the public sector's preparedness to respond, or its recovery activities involving the support of disaster affected communities in the restoration of services, reconstruction of physical infrastructure and restoration of emotional, social, economic and physical wellbeing following terrorist incidents. An examination of the structures, arrangements or activities established under the emergency management approach would have diverted the focus of the audit from arrangements introduced by the government to specifically address the effects of terrorism on essential services and critical infrastructure.

1.3 Conclusion

Victoria was the first Australian jurisdiction to develop arrangements for protecting essential services from the effects of terrorism, including at the national level. Victoria has played a significant part in developing capability for protecting essential services and critical infrastructure, nationally and in other states, in particular the capability development of crisis centres of other states and territories.

The government has invested around $255 million in counter-terrorism initiatives, since 2002, to protect the community against terrorism including prevention, response and recovery. Victoria Police, emergency services, health services and other government agencies have been provided with new tools to combat terrorism and its consequences.

The establishment of a governance structure comprising the Security and Emergencies Committee of Cabinet, the Central Government Response Committee, Government Security and Continuity Network Coordination Group (G-SCN-CG) and Security and Continuity Networks (SCNs) to underpin the arrangements for protecting essential services and critical infrastructure is a positive initiative. However, the governance arrangements could be more effective:

- The co-existence of Part 6 of the Act for essential services and the CIP framework for critical infrastructure is confusing to agencies and hinders coordination.
- SCNs are not fully operational with varying levels of progress. Two of the nine are operating well, one other has recently converted to the SCN format after operating for some time under other arrangements. Two are in the early stages of operation. Another held its first meeting in October 2008. The remaining three have not been established. Timeframes for implementation of the CIP framework have not been set.
- The effectiveness of the G-SCN-CG has been reduced by the delayed development of the SCNs and the co-chairing arrangements between the Department of Premier and Cabinet (DPC) and Victoria Police. The requirement under the arrangements for the G-SCN-CG to focus on the CIP framework rather than both critical infrastructure and essential services has limited its potential effectiveness.

- Respective roles and responsibilities of agencies involved are unclear, particularly in the CIP framework.
- Efforts to identify and mitigate inter-agency risks associated with joined-up arrangements for managing the framework were not evident.
- An adequate performance measurement and monitoring framework has not been developed.

Governance arrangements to assist owners/operators of critical infrastructure and operators of declared essential services to prepare to respond to terrorism incidents are at different stages of development across sectors. In the absence of an overarching performance monitoring framework success in implementing Part 6 of the Act and the CIP framework is difficult to measure.

Three departments audited have 'declared' essential services under the *Terrorism (Community Protection) Act 2003* (the Act). The sectors managed by these three departments—energy, transport and water—are the most significant industry sectors in terms of providing for business continuity and the state's ability to recover from a terrorist incident. The alternative arrangements in place for the police and emergency services sector to prepare to respond to terrorism incidents are considered reasonable.

As departments in the remaining sectors have yet to consider whether such declarations are necessary, we were unable to gain assurance whether all essential services have been declared.

Three lead departments were not aware of the critical infrastructure listed on the critical infrastructure register for their industry sectors. This inhibits their ability to work with owners/operators to encourage them to take up the recommended practices identified in the CIP framework.

There is a requirement for risk management plans of declared essential services to be audited annually and annual audits of risk management plans for critical infrastructure are encouraged. However, what would constitute such an audit has not been defined. Similarly there is no guidance on the qualifications required of an auditor who can audit the plans.

Apart from a 'lessons learned' database that is maintained by Victoria Police and records the outcomes of all NCTC coordinated exercises, there was little evidence of a systemic capacity to capture information about training exercises conducted under Part 6 of the Act and the CIP framework. The lack of a central repository for exercise reports makes collective analysis of outcomes difficult. We saw no evidence of strategic analysis of recommendations and consequently, it is not apparent that reports are driving continuous improvement.

It is clear from the government's policy document *Enhancing Victoria's Domestic Security: New measures for the fight against terrorism* that DPC has responsibility to coordinate Victoria's major incident management, including for counter-terrorism policy and planning. While responsibility for oversight of operators of declared essential services in specific sectors rests with the relevant minister and department, DPC should exercise firmer leadership in administering Part 6 of the Act and implementation of the CIP framework and remove barriers to their effective implementation.

Since the emergence of national arrangements, subsequent to introduction of the 2003 Victorian legislation, and given the issues identified during the audit, it is timely to review the arrangements for protecting the state's essential services and critical infrastructure. Such a review should aim to reduce the complexity of the state's arrangements and streamline practices, consistent with maintaining regulation and coordination to mitigate risks specific to our highly privatised service delivery environment.

DPC has advised it intends to examine Victoria's critical infrastructure protection arrangements including Part 6 of the Act and the CIP framework and to assess their effectiveness and appropriateness for the near to medium term.

1.4 Recommendations

The Department of Premier and Cabinet should:

- establish clear oversight and coordination of the arrangements for both Part 6 of the *Terrorism (Community Protection) Act 2003* and the CIP framework by an appropriate body, such as the Government Security and Continuity Network Coordination Group with expanded responsibilities **(Recommendation 4.1)**
- lead the development of a performance management framework for measuring, monitoring and reporting on the implementation of Part 6 of the Act and the CIP framework. The framework should include key indicators, targets and reporting arrangements for assessing the extent to which departments, agencies and industry have fulfilled their obligations, as well as measures for monitoring achievement of joint objectives **(Recommendation 4.2)**
- clarify the roles and responsibilities of departments and agencies under Part 6 of the Act and CIP framework to reduce confusion and gaps **(Recommendation 4.3)**
- provide definitive guidance on identifying essential services for declaration to better inform relevant departments in discharging their responsibilities under Part 6 of the Act **(Recommendation 4.4)**
- identify risks arising from the joined-up nature of the approach to protecting essential services and critical infrastructure, and to assist departments and agencies to develop associated risk management arrangements at the whole-of-government level **(Recommendation 4.5)**
- clarify the requirements in relation to establishing Security and Continuity Networks in designated sectors, so that there is a shared understanding of those requirements. **(Recommendation 4.6)**

Representatives of lead departments should obtain necessary security clearances so appropriate officers can access information relevant to their sectors. **(Recommendation 4.7)**

The Department of Premier and Cabinet, in consultation with Victoria Police, should develop clear guidance to distinguish between declared essential services and critical infrastructure to assist departments, Victoria Police and industry in implementing Part 6 of the Act and the CIP framework more effectively. **(Recommendation 5.1)**

The Department of Premier and Cabinet should provide clear guidance on terms such as ‘audit’, ‘auditor’ and ‘adequacy of the exercise’ to assist departments, Victoria Police and industry to implement requirements more reliably. **(Recommendation 5.2)**

The Department of Premier and Cabinet and Victoria Police, in consultation with departments, should standardise reporting on training exercises conducted under Part 6 of the Act and the CIP framework to promote greater consistency and to enable better identification of lessons learned and continuous improvement. **(Recommendation 5.3)**

Reports on the training exercises should be retained in an appropriately secured central repository so that consolidated results of the exercises can be drawn together effectively. **(Recommendation 5.4)**

2 Audit Act 1994 Section 16— submissions and comments

2.1 Introduction

In accordance with section 16(3) of the Audit Act 1994 a copy of this report, or relevant extracts from the report, is provided to the head of each agency involved in the audit with a request for comments or submissions.

Comments or submission received within 10 business days must be included in the report. The comments and submissions provided are not subject to audit nor the evidentiary standards required to reach an audit conclusion. Responsibility for their accuracy, fairness and balance rests solely with the agency head.

2.2 Submissions and comments received

***RESPONSE* provided by Chief Commissioner, Victoria Police**

The recommendations in the VAGO Report are supported.

It is the view of Victoria Police that:

- *The Department of Premier and Cabinet develops policy and framework relative to critical infrastructure, and*
- *Victoria Police is responsible for the implementation and application of critical infrastructure protection.*

This partnership approach is in accordance with counter-terrorism and policing arrangements and has worked quite well in regard to critical infrastructure protection. Accordingly, it is recommended that these arrangements do not change however, in light of VAGO's report, consideration should be given to modernising arrangements concerning critical infrastructure protection and declared essential services.

The Victoria Police and the Department of Premier and Cabinet have worked tirelessly in a partnership approach to ensure the best standards of critical infrastructure protection but at all times the potential for doing even better has been the mind set. With that in mind, the VAGO Report should be embraced by both Victoria Police and the Department of Premier and Cabinet.

***RESPONSE* provided by Secretary, Department of Human Services**

While operating within the provisions of the Act and the CIP framework, the Department believes that work it has undertaken with the health sector, a key emphasis on planning within an "all hazards" framework does provide a comprehensive approach.

The Department is currently in the process of securing a list of health related critical infrastructure from the Victoria Police register and also establishing a process to provide further guidance to the co-ordination of critical infrastructure within the health portfolio.

The Department will be an active participant in any action taken with respect to a review of the CIP framework.

***RESPONSE* provided by Secretary, Department of Justice**

The emergency services sector places great importance on ensuring that redundancy, continuity of services and surge capacity are part of core business. These are key elements of emergency management and the sector actively pursues opportunities for continuous improvement. I am confident that the sector has, and will continue to, work together to ensure that Victoria's ability to manage emergencies, including emergencies arising from act/s of terrorism, is a priority.

***RESPONSE* provided by Secretary, Department of Primary Industries**

Officers of the Victorian Auditor-General's Office have consulted extensively with the relevant officers in the Department of Primary Industries in preparing this report. The facts contained in the report are correct and the context has been represented fairly.

***RESPONSE* provided by Secretary, Department of Sustainability and Environment**

I am satisfied that the findings of this report reflect the performance of the water sector in meeting its obligations under the Terrorism (Community Protection) Act 2003 and the Victorian Framework for Critical Infrastructure Protection from Terrorism.

***RESPONSE* provided by Secretary, Department of Transport**

I understand that Victoria has a spectrum of solutions for improving preparedness of industry for terrorism, extending from legislation to voluntary guidelines to industry self management. Different approaches at various points along this spectrum are employed, depending on the threat and risk context, industry regulatory framework, assessed criticality and vulnerability. Hence there will rarely be identical approaches across government to enhancing the preparedness of different industries or industry sectors.

While noting your comments on the Terrorism (Community Protection) Act 2003, DOT views the Act and its associated Regulations as providing appropriate and clear mechanisms for the purposes of Part 6.

I also note that the Government Security and Continuity Network Coordination Group (G-SCN-CG) is primarily a communications mechanism between individual Security and Continuity Networks. It is not an executive forum of Government and appears to have no existence within the Act. Therefore, the G-SCN-CG may not be an appropriate forum to advise relevant Ministers or departments on application of the Act. With reference to the operating principles at page 27 to your report, individual roles and responsibilities could be exercised by G-SCN-CG members provided that they act in concert.

RESPONSE provided by Acting Secretary, Department of Premier and Cabinet

The Department of Premier and Cabinet (DPC) agrees with your findings that a review of the critical infrastructure arrangements is warranted and, to that end, a review has already commenced. The terms of reference of this review includes consideration of your findings and recommendations. DPC has also recommended to the Commonwealth that a review of the national arrangements is warranted. This suggestion has received strong support from other States and Territories.

The Acting Secretary DPC provided detailed comments elaborating on the report, together with a response to the audit recommendations. Due to its length, the additional response is provided in Appendix C of this report.

2.3 Audit observations

The response by the Acting Secretary, Department of Premier and Cabinet provides further useful context, especially regarding activities prior to the introduction of the 2003 legislation. However, at some points it misconstrues the wording of the report and the recommendations. This is disappointing given the protracted nature of discussions with departmental representatives and endeavours to accommodate departmental views and context without compromising the integrity of the report.

In particular the report does not recommend ‘seeking declaration of further essential services’. The recommendation is that more definitive guidance be provided on how to determine what constitutes an essential service that should be declared. This would better assure completeness and reliability of planning as well as complementarity and consistency of responses should an incident occur.

Further, Audit does not advocate an ‘operational role’ for the department, beyond that of a department servicing its Minister in administering legislation. Specifically Audit considers the department is responsible for ascertaining that the provisions of the Act are reasonably assured of operating predictably and as intended. This requires some central oversight and monitoring, not least to identify the type of difficulties in interpretation and inconsistencies in operation of the Act that have been identified by this audit.

With regard to the response by the Secretary, Department of Human Services, the report acknowledges the ’all hazards, all agencies‘ approach, but notes the added risks associated with utilising different frameworks in a broader emergency context and considers this warrants particular and prospective consideration.

Overall Audit considers most elements of the state’s preparedness to respond to terrorism incidents are satisfactory. Particular aspects have however been identified as requiring attention to better assure a cohesive and complementary approach should an incident occur.

3 Background

The terrorist attacks in the United States in 2001 introduced a new and confronting dimension to the international security environment. Later attacks in Bali, Madrid, Jakarta and London confirmed that the terrorism threat is not limited to the United States. While Australia has not been directly attacked by terrorists in recent times, its citizens and interests have been attacked offshore.

Since 2001, Australia's national counter-terrorism alert has been at the 'medium' level, meaning a terrorist attack within Australia could occur. The heightened security environment has prompted changes in security arrangements at the national, state and territory levels.

At the April 2002 Leaders' Summit on Terrorism and Multi-jurisdictional Crime, all states and territories agreed to review their legislation and counter-terrorism arrangements to ensure that they were effective enough to deal with the terrorism threat.

3.1 Counter-terrorism arrangements

3.1.1 National arrangements

Australia's counter-terrorism capability operates through a cooperative partnership between national, state and territory jurisdictions, with joint responsibility for developing and maintaining nationwide capability. The Commonwealth has the national coordination responsibility.

The National Counter-Terrorism Committee (NCTC) has driven the development of the national approach to prepare for, respond to, and recover from potential terrorist attacks. Commonwealth, state and territory representatives make up the NCTC, which, among other things, is responsible for maintaining the national counter-terrorism plan. The plan sets out Australia's high-level strategy for preventing and dealing with acts of terrorism in Australia and its territories. It addresses capability—prevention, preparedness, response and recovery—policy development, coordination and strategic arrangements.

In June 2004 the Council of Australian Governments endorsed the NCTC's *National Guidelines for Protecting Critical Infrastructure from Terrorism* (the national CIP framework) as part of broader national counter-terrorism arrangements. Victoria contributed significantly to the development of the national CIP framework.

Victoria's activities are closely linked to the national framework through aligned counter-terrorism policies and arrangements, intergovernmental and industry committees and plans.

3.1.2 Victorian arrangements

'All hazards, all agencies' approach to emergency management

Victoria's emergency management arrangements are based on a common set of arrangements for all emergencies known as the 'all hazards, all agencies' approach. Under this approach all emergencies, regardless of their cause, are managed through emergency management arrangements set out in the *Emergency Management Act 1986*, the *Emergency Management Manual Victoria* and the *State Emergency Response Plan*. This means that the same agencies and arrangements used to respond to routine incidents and emergencies are also used to respond to terrorism incidents.

The *Emergency Management Act 1986*, the *Emergency Management Manual Victoria* and the *State Emergency Response Plan* allocate roles and responsibilities and provide an organised structure to facilitate planning, preparedness, operational coordination, and nominated control agencies for response and for community recovery from emergency situations faced by the Victorian population.

The arrangements have been tested through events such as the Longford gas crisis, and refined in the lead-up to major events such as Y2K, the 2000 World Economic Forum in Melbourne and the 2006 Commonwealth Games.

Victoria's early response to the terrorism threat

The 11 September 2001 terrorist attacks in New York and Washington and the subsequent October 2002 Bali bombings prompted reform and enhancement of the national and Victorian counter-terrorism arrangements, through the introduction of new arrangements and legislation and the improvement of counter-terrorism capabilities.

In November 2002 the Victorian government released its counter-terrorism policy statement *Enhancing Victoria's Domestic Security: New measures for the fight against terrorism*. The policy statement included requirements for Victoria Police to assist operators of essential services relating to electricity, gas, water, transport and fuel, in the development, validation and audit of their risk management plans and the coordination of joint exercises.

In 2003, the *Terrorism (Commonwealth Powers) Act 2003* and the *Terrorism (Community Protection) Act 2003* were introduced, establishing new counter-terrorism powers, including provisions for the protection of declared essential services. Victoria is the only jurisdiction to introduce essential services protection legislation.

The government subsequently released two further policy documents:

- *Protecting our Community: Attacking the Causes of Terrorism* in September 2005
- *A Safer Victoria—Protecting our Community: New Initiatives to Combat Terrorism* in October 2006.

3.2 Essential services and critical infrastructure

Protecting essential services and critical infrastructure is integral to minimising the impact and consequences of a terrorist attack. Victoria was an early starter in developing its approach to critical infrastructure protection. The approach was influenced by the government's response to the Longford gas crisis of 1998 and by the fact that much of the state's essential services and critical infrastructure is privately owned or operated.

Essential services

For the purposes of Part 6 of the *Terrorism Community Protection Act 2003* (the Act), 'essential services' means transport, fuel (including gas), light, power, water and sewerage services, and any other service declared to be an essential service by the Governor-in-Council under the Act. The Act mandates operators of 'declared' essential services to be involved in planning for:

- the protection of those services from the effects of terrorist acts
- responding to and recovering from an attack
- the continued safe operation of the service in the event of an attack.

Under the Act operators of declared essential services are required to:

- prepare risk management plans to prevent and mitigate risks to the service, to aid recovery and service continuity in the event of a terrorism incident
- have the risk management plans audited annually
- participate in annual training exercises to test their risk management plans.

Part 6 was designed to encourage partnership between Victorian Government departments, Victoria Police and operators of essential services.

Critical infrastructure

The arrangements in the Act are supported by the *Victorian Framework for Critical Infrastructure Protection from Terrorism* (the CIP framework), published in April 2007, which sets out the guiding principles and coordination arrangements for government and industry to develop joint strategies for protecting Victoria's critical infrastructure. Among other things, the CIP framework formalised the involvement of Victoria Police in the validation and audit of risk management plans and the coordination of joint exercises for critical infrastructure.

Under the CIP framework, critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of Victoria and its community. Victoria has adopted the national definition of critical infrastructure.

The Victorian CIP framework draws on the national CIP framework introduced in 2004, and other nationally agreed documents for critical infrastructure protection, and is consistent with the national CIP framework. Under the CIP framework, owners/operators of critical infrastructure are encouraged to comply with the same practices required of operators of declared essential services, by preparing risk management plans, and auditing and testing those plans.

While the requirements under the Act for operators of declared essential services are mandatory, under the CIP framework compliance by owners/operators of critical infrastructure is voluntary. As such, the CIP framework relies upon partnerships between government and industry, to create and implement a cooperative culture of security protection and awareness.

Testing preparedness

Counter-terrorism and emergency management is the subject of exercising and review, both within Victoria and nationally, including specific exercises for transport infrastructure and dealing with mass casualties. While training exercises under Part 6 of the Act and the CIP framework are primarily designed to test the operation of the risk management plan of operators of essential services and owners/operators of critical infrastructure respectively, the focus of Victoria's counter-terrorism and emergency management exercises is on the capability of emergency management agencies to save lives and property.

Committees, networks and key office holders

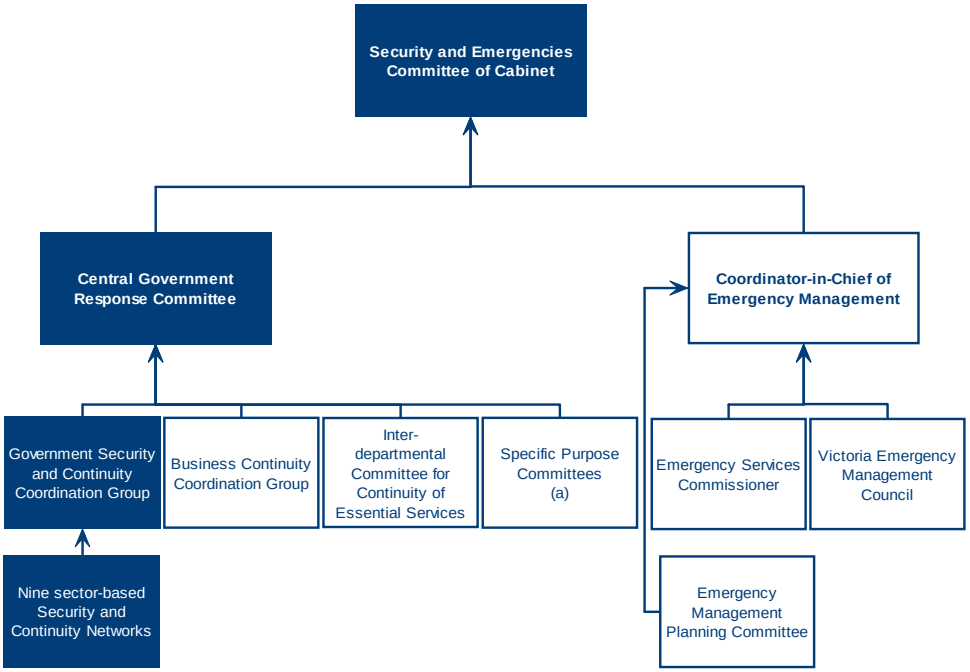
The Act and the CIP framework operate within Victoria's 'all hazards, all agencies' emergency management arrangements.

A range of committees and networks oversee and coordinate Victoria's emergency management arrangements. These include, at the highest level, the Security and Emergencies Committee of Cabinet and the Central Government Response Committee.

Coupled with the committees and networks designed to implement the state's 'all hazards, all agency' emergency management arrangements are other committees and networks specifically established to assist the government and industry sectors to mitigate the risks to infrastructure from terrorism incidents. These include the Government Security and Continuity Network Coordination Group and Security and Continuity Networks.

Figure 3A shows the committees, networks and key office holders that oversee and coordinate Victoria's emergency management arrangements. The shaded components are those which in practice relate to the protection of critical infrastructure and declared essential services from the effects of terrorism incidents.

Figure 3A
Victoria's emergency management arrangements—committees, networks and key office holders



Note: (a) Specific Purpose Committees are established on as needs basis.
Source: Emergency Management Manual Victoria and information provided by the Department of Premier and Cabinet.

Under the arrangements, a Security and Continuity Network is not a network to be used in the event of an emergency, but rather is a network established to consider security, emergency management and business continuity policies and practices relating to a specific Victorian critical infrastructure sector.

A chart setting out the roles and responsibilities and membership of the groups associated with the protection of infrastructure is included in Part 4 of this report.

Agency involvement

The Premier and consequently the Department of Premier and Cabinet (DPC) has responsibility for administering Part 6 of the Act. DPC also has a leadership role under the CIP framework in developing and coordinating whole-of-government strategy and policy for critical infrastructure protection to ensure a consistent approach across government. Victoria Police has key roles in relation to Part 6 of the Act and the CIP framework. Other departments also have important roles in ensuring operation of arrangements aimed at protecting declared essential services and critical infrastructure. Departments have been allocated responsibility for working with specific industry sectors under the CIP framework.

Funding government counter-terrorism initiatives

Since 2002–03, the government has allocated around $255 million to counter-terrorism initiatives. Initiatives include establishing the Security and Emergencies Unit within DPC to coordinate Victoria's major incident management; the Critical Infrastructure Protection Unit in Victoria Police to assist in the assessment of potential risks to essential services; and the State Crisis Centre to support the government while it manages severe emergencies, including terrorism incidents. Further details of funded initiatives can be found in Appendix A to this report.

3.3 Audit objective and scope

The objective of the audit was to examine the state's preparedness to respond to terrorism incidents, relating to essential services and critical infrastructure.

In scope

The audit examined the governance arrangements established to assist operators of essential services and owners/operators of critical infrastructure to respond to terrorism incidents. The activities of selected Victorian government agencies with roles and responsibilities under Part 6 of the Act and the CIP framework were examined, including how they consulted and interacted with owners/operators of critical infrastructure and operators of declared essential services.

We examined:

- whether there is a clear governance structure in place that specifies roles, responsibilities and lines of accountability of key state agencies
- whether selected government entities and owners and operators of declared essential services and critical infrastructure comply with Part 6 of the *Terrorism (Community Protection) Act 2003* and the *Victorian Framework for Critical Infrastructure Protection From Terrorism* respectively; and have established processes to assist in the implementation of these requirements
- funding for counter-terrorism initiatives including for preventing, responding to and recovering from terrorist attacks.

The principal agencies examined were Victoria Police and DPC, including the operations of the State Crisis Centre. The audit also included the departments of:

- Human Services
- Innovation, Industry and Regional Development
- Justice
- Primary Industries
- Sustainability and Environment.
- Transport (formerly the Department of Infrastructure).

Out of scope

Because of the focus of the audit on response, it did not examine:

- prevention activities involving collecting, analysing and disseminating intelligence about terrorist intentions and capabilities
- the implementation of additional powers to police, mandatory reporting of theft or loss of specified chemicals and substances, or the protection of counter-terrorism information introduced in the *Terrorism (Community Protection) Act 2003*.

Given the audit scope, the audit did not examine the state's broader emergency management arrangements. Nor did it consider the public sector's preparedness to respond, or its recovery activities involving the support of disaster affected communities in the restoration of services, reconstruction of physical infrastructure and restoration of emotional, social, economic and physical wellbeing following terrorist incidents. An examination of the structures, arrangements or activities established under the emergency management approach would have diverted the focus of the audit from arrangements introduced by the government to specifically address the effects of terrorism on essential services and critical infrastructure.

The Department of Primary Industries' identification and management of biosecurity risks for Victoria's livestock industry and associated risks was not examined. These matters were the subject of the performance audit of *Biosecurity Incidents: Planning and Risk Management for Livestock Diseases* tabled in Parliament in November 2008.

3.4 Audit criteria and method

The criteria were drawn from relevant legislation, guidelines, policies and procedures statements, and standards. In addressing the criteria, this audit examined:

- governance aspects of the related state agencies including their roles, responsibilities, and coordination and leadership arrangements
- the arrangements established by selected departments and agencies for monitoring the preparedness and capability of the operators of declared essential services and owners/operators of critical infrastructure to respond to terrorism incidents
- records relating to the funding of major counter-terrorism initiatives including for preventing, responding to and recovering from terrorist attacks.

Key personnel were consulted, documentation reviewed at the selected departments and agencies, and in relation to committees and networks including the Security and Emergencies Committee of Cabinet, the Central Government Response Committee, the Government Security and Continuity Network Coordination Group, and Security and Continuity Networks. Agencies in other jurisdictions were consulted to gauge the level of Victoria's involvement in the national arena and to observe arrangements for the protection of essential services and critical infrastructure.

The audit was conducted in accordance with the Australian Auditing Standards applicable to performance audits, and included tests and procedures sufficient to enable audit conclusions to be reached.

The total cost of the audit was $510 000 and includes staff time, overheads and printing.

4 Governance

At a glance

Background

Following 11 September 2001, the Victorian government reappraised the state's vulnerability to terrorist attack and its capacity to respond to a major emergency. To address the protection of essential services against the effects of terrorist acts, the government established the *Terrorism (Community Protection) Act 2003* (the Act). In April 2007, the *Victorian Framework for Critical Infrastructure Protection from Terrorism* (the CIP framework) was introduced.

The Act and the CIP framework establish the roles and responsibilities of government and owners and operators for protecting declared essential services and critical infrastructure. Where multiple agencies and industry are required to work together, clear governance arrangements are need to achieve shared objectives.

Key findings

- Victoria acted early to develop the means to protect essential services and critical infrastructure following the 2001 terrorist attacks.
- The co-existence of Part 6 of the Act for essential services and the CIP framework for critical infrastructure is complex and challenging for agencies. This co-existence creates confusion, and affects coordination between agencies.
- Efforts to identify and mitigate inter-agency risks associated with joined-up arrangements for managing essential services and critical infrastructure were not evident.
- The establishment of forums for communicating to government, across government and with industry is a positive initiative. However delays in establishing Security and Continuity Networks (SCNs), unclear responsibilities of lead departments, and a range of issues affecting the operations of the Government Security Continuity Network Coordination Group have affected the ability of the governance arrangements to operate with maximum benefit.

At a glance – *continued*

Key findings – *continued*

- SCNs are at varying levels of development: two of the nine are operating well, one other has recently converted to the SCN format after operating for some time under other arrangements. Two are in the early stages of operation. Another held its first meeting in October 2008. The remaining three have not been established. The Department of Premier and Cabinet (DPC) needs to review and resolve whether designated industries should establish SCNs.
- An adequate framework for measuring and monitoring overall performance for the implementation of Part 6 of the Act and the CIP framework has not been developed.

Key recommendations

The Department of Premier and Cabinet should:

- establish clear oversight and coordination of the arrangements for both Part 6 of the *Terrorism (Community Protection) Act 2003* and the CIP framework by an appropriate body, such as the Government Security and Continuity Network Coordination Group with expanded responsibilities **(Recommendation 4.1)**
- lead the development of a performance management framework for measuring, monitoring and reporting on the implementation of Part 6 of the Act and the CIP framework. The framework should include key indicators, targets and reporting arrangements for assessing the extent to which departments, agencies and industry have fulfilled their obligations, as well as measures for monitoring achievement of joint objectives **(Recommendation 4.2)**
- clarify the roles and responsibilities of departments and agencies under Part 6 of the Act and CIP framework to reduce confusion and gaps **(Recommendation 4.3)**
- provide definitive guidance on identifying essential services for declaration to better inform relevant departments in discharging their responsibilities under Part 6 of the Act **(Recommendation 4.4)**
- identify risks arising from the joined-up nature of the approach to protecting essential services and critical infrastructure, and to assist departments and agencies to develop associated risk management arrangements at the whole-of-government level **(Recommendation 4.5)**
- clarify the requirements in relation to establishing Security and Continuity Networks in designated sectors, so that there is a shared understanding of those requirements. **(Recommendation 4.6)**

Representatives of lead departments should obtain necessary security clearances so appropriate officers can access information relevant to their sectors. **(Recommendation 4.7)**

4.1 Introduction

Arrangements under the *Terrorism (Community Protection) Act 2003* (the Act) and the *Victorian Framework for Critical Infrastructure Protection from Terrorism* (CIP framework) establish the roles and responsibilities of related government agencies, committees and owners and operators for protecting declared essential services and critical infrastructure. Victoria's arrangements for protecting essential services and critical infrastructure against a possible terrorist attack rely upon coordination between multiple parties from the public sector and industry to work together to achieve an effective outcome. Given this, it is important that government agencies work together in a 'joined-up' way, and that agencies establish strong relationships with the industry sectors with which they work.

Where multiple parties are required to work together to achieve shared outcomes, it is fundamental that roles and responsibilities, communication and coordination arrangements, risk management and performance monitoring are clearly set out and understood by all parties.

4.2 Roles and responsibilities

The arrangements to provide for the protection of declared essential services and critical infrastructure were assessed to determine whether the roles and responsibilities and accountabilities of the various parties are clearly defined and understood.

4.2.1 The differential approaches

There are two components of Victoria's arrangements for protecting the state's essential services and infrastructure from the effects of terrorism incidents.

While Part 6 of the Act has mandatory requirements for operators of declared essential services, there is no equivalent force of law for the CIP framework for owner/operators of critical infrastructure. Take-up of the practices is voluntary for owners/operators. Accordingly there are no penalties for non-compliance.

This absence of the force of law has affected the sharing of information between owners/operators of critical infrastructure, Victoria Police and the departments designated to work with their industry (lead departments). For example, an owner/operator of critical infrastructure is not compelled to provide a copy of a risk management plan to its lead department or Victoria Police under the CIP framework. Under the Act, operators of declared essential services are required to provide a copy of a risk management plan to the relevant minister/department. The 'light handed' approach of the CIP framework, adds unnecessary complexity to the ability of Victoria Police and lead departments to encourage an appropriate level of preparedness to respond to terrorism incidents by operators/owners of critical infrastructure. Neither Victoria Police, nor departments, can access risk management plans to assess the

extent to which risks have been mitigated unless an owner/operator agrees to provide that access.

The roles and responsibilities of government departments and agencies are different under the Act and the CIP framework. For example:

- under the Act, 'relevant' departments are responsible for recommending the essential services to be declared, for establishing timeframes for operators to prepare risk management plans, and determining when and in which manner training exercises to test risk management plans are to occur
- under the CIP framework:
  - Victoria Police is responsible for identifying critical infrastructure and owner/operators are responsible for determining when they will conduct exercises and whether they will operate in compliance with recommended practices.
  - 'Lead' departments are responsible for working with industry to encourage adoption of practices.

The different approaches lead to confusion for agencies and affects coordination between agencies. It is not clear why there are two sets of arrangements. There is merit in reviewing these arrangements.

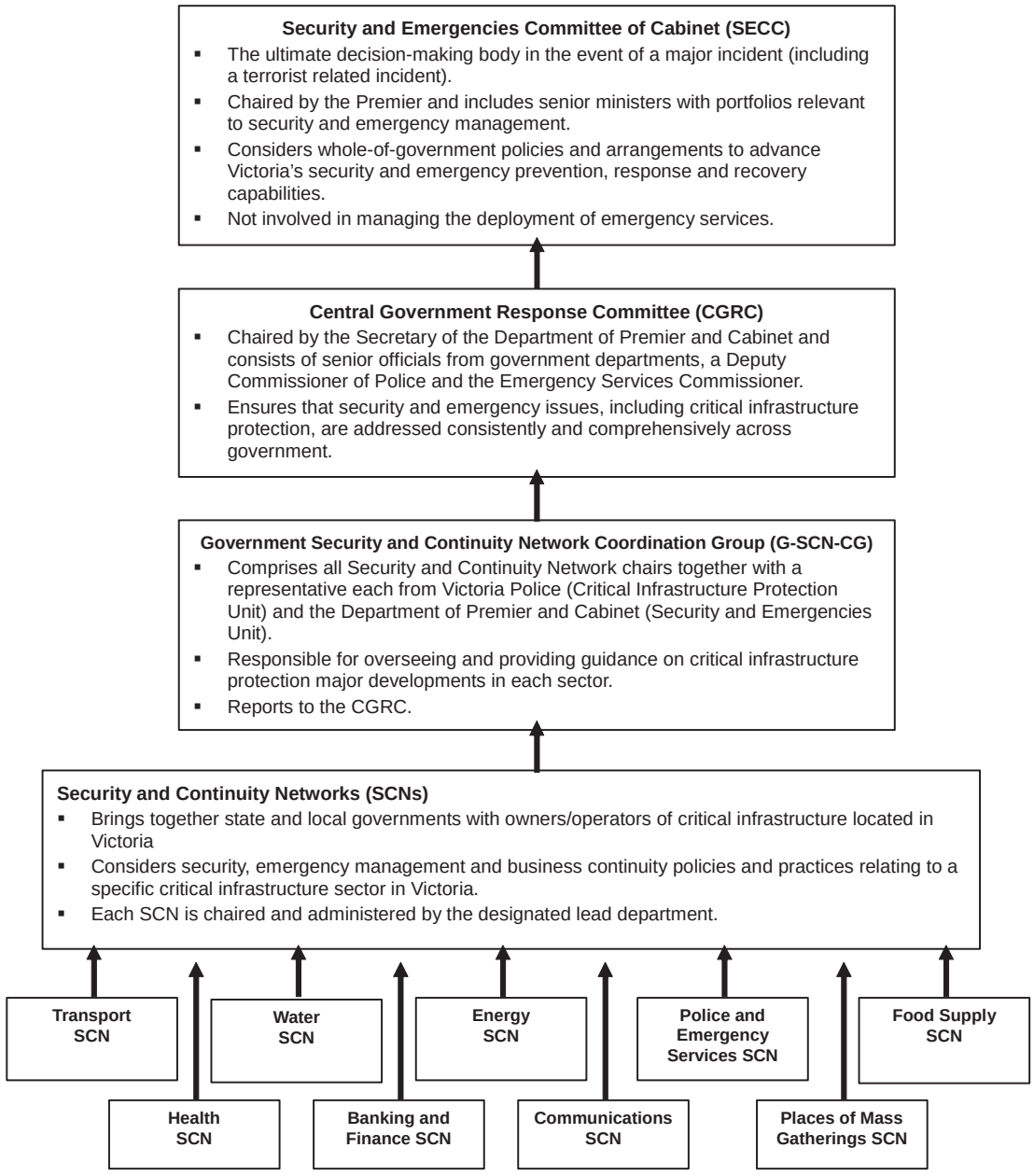
This situation appears attributable to Victoria being an early proponent in developing the counter-terrorism arrangements both within the state and nationally. However, since the emergence of national arrangements, subsequent to the introduction of the 2003 Victorian legislation, it is now timely to review the arrangements. Such a review should aim to reduce the complexity of the arrangements and streamline practices, consistent with maintaining appropriate regulation and coordination to mitigate risks specific to our highly privatised service delivery environment.

Following feedback by VAGO during the audit, the Department of Premier and Cabinet (DPC) advised that it intends to examine Victoria's critical infrastructure protection arrangements including Part 6 of the Act and the CIP framework and to assess their effectiveness and appropriateness for the near to medium term.

4.2.2 Committees and networks

There is a cascading system of committees and networks related to the protection of declared essential services and critical infrastructure. Figure 4A sets out their roles and responsibilities, relationships and memberships.

Figure 4A
Governance arrangements for Victoria's critical infrastructure protection



Source: Department of Premier and Cabinet, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007 and information provided by audited agencies.

Security and Emergencies Committee of Cabinet

The state's most senior security coordination body is the Security and Emergencies Committee of Cabinet (SECC). It is responsible for providing direction, policy development and oversight for the implementation of strategies and programs affecting security and emergency management issues. The SECC is chaired by the Premier and includes a number of senior ministers with portfolios relevant to security and emergency management.

For the period from December 2002 to May 2008, agenda items related to counter-terrorism and the critical infrastructure framework were not routinely followed up. There were instances where updates and briefings requested by the SECC were not provided at subsequent meetings. For example:

- In July 2004, although the SECC endorsed the development of the Framework of a State-wide Strategic Risk Assessment on Terrorism for consideration at a future meeting of SECC, this matter was not reported back to SECC.
- In November 2005, SECC agreed that further advice on the outcome of the Mercury 05 exercise, (a multi-jurisdictional counter-terrorism exercise conducted under the auspices of the National Counter-Terrorism Committee) should be provided to it once assessment of the exercise had been completed. Although a debrief report was subsequently prepared by the Commonwealth Attorney-General's Department, the SECC did not obtain a copy of the debrief report.

Central Government Response Committee

The SECC is supported by the Central Government Response Committee (CGRC), chaired by the Secretary of DPC. The CGRC comprises a Deputy Secretary level representative from each department, a Deputy Commissioner of Victoria Police, the Department of Human Services' Recovery Coordinator and the Victorian Emergency Services Commissioner. The CGRC's role includes ensuring that security and emergency issues, including critical infrastructure protection, are addressed consistently and comprehensively across government.

Instances were identified where action/agenda items related to essential services and critical infrastructure protection were not followed up. For example:

- At the August 2004 meeting, departments were requested to provide submissions on the effectiveness of Part 6 of the Act by October 2004. At the October 2004 meeting, DPC reported that Part 6 of the Act was being reviewed, and that recommendations would be presented to the CGRC before seeking approval of the SECC. There was no future reference to this review or the submissions at subsequent meetings of the CGRC.
- At the November 2005 meeting, the debriefing for the Mercury 05 exercise was postponed. A verbal debrief was provided to CGRC at the January 2006 meeting with DPC indicating that a final report would be provided to CGRC for consideration when complete. A final report was prepared but there was no reference to the report at subsequent CGRC meetings.

Following feedback provided by VAGO during the audit, the secretariat introduced a rolling action list for the CGRC agenda to ensure minuted items are actioned.

Government Security and Continuity Network Coordination Group

The Government Security and Continuity Network Coordination Group (G-SCN-CG) is comprised of the Chairs of all Security and Continuity Networks (SCNs), a representative from Victoria Police's Critical Infrastructure Protection Unit (CIPU) and a representative from the DPC's Security and Emergencies Unit (SEU).

Its role includes oversight of the SCNs, producing guidance on critical infrastructure protection developments in each sector, and reporting to the CGRC on the operation of the networks. The operating principles of the G-SCN-CG are to:

- provide whole-of-government coordination in developing and implementing the CIP framework
- ensure that critical infrastructure in Victoria is adequately identified, criticality determined and ranked
- support Victoria Police in maintaining the Victorian critical infrastructure database up to date and relevant
- ensure that owners/operators of critical infrastructure are supported in their security, emergency and risk management planning to enable continuity of service through the SCNs
- encourage private sector owners/operators and require the government sector to develop relevant capabilities to ensure continuity of service
- facilitate the establishment of SCNs for every critical infrastructure sector
- support SCNs as necessary on any matter pertaining to security, emergency management, business continuity or risk management of any sector
- provide strategic direction to SCNs on the risk management of critical infrastructure and interdependencies
- provide strategic oversight of developments and status activities in all SCN sectors and report back to the CGRC.

The G-SCN-CG is co-chaired by Victoria Police's CIPU and DPC's SEU with the SEU providing secretariat support.

The SEU has taken the dominant role in co-chairing the G-SCN-CG, with Victoria Police taking a lesser role. There is a need to improve the way that both the SEU and CIPU co-chair and service the G-SCN-CG. Equal input to co-chairing the G-SCN-CG by Victoria Police would provide greater opportunity for better coordination between the arrangements for protecting essential services and critical infrastructure as DPC is responsible for administering Part 6 of the Act which relates to essential services, and Victoria Police is responsible for identifying and prioritising critical infrastructure under the CIP framework.

The G-SCN-CG's effectiveness could be improved by:

- clarifying the co-chairing roles of DPC (SEU) and Victoria Police (CIPU)
- better servicing by DPC and Victoria Police. This should include developing a plan that outlines the group's objectives, strategies and milestones, and monitoring implementation of the plan
- establishing a timetable for implementing the CIP framework and requiring lead departments to report progress against the timetable
- expanding its role to oversee and provide guidance for implementing Part 6 of the Act for declared essential services
- clarifying departmental responsibilities for critical infrastructure sectors. Currently detailed statements of department and agency responsibilities under the CIP framework, are not aligned with overarching statements of those responsibilities, creating confusion and allowing gaps in responsibilities to exist
- defining a number of terms under CIP framework and the Act (further detail is provided in Part 5 of this report).

During the audit we noted an absence of follow up, and reporting back on, action items at subsequent meetings. Following discussion with the audit team, the G-SCN-CG acted to resolve several long-standing agenda items.

Security and Continuity Networks

Consistent with national arrangements, Victoria has adopted a sector approach to the management of critical infrastructure. Under this approach, critical infrastructure sectors are linked to lead departments so that industry and government can develop relationships and work together in partnership to create a culture of security awareness and protection. The critical infrastructure sectors have also been aligned to the national approach to avoid confusion between the state and national arrangements.

Figure 4B sets out the Victorian critical infrastructure sectors and related lead departments.

Figure 4B
Victorian critical infrastructure sectors, sub-sectors and lead departments

Sector	Sub-sectors	Lead department
Energy	Gas, petroleum fuels, electricity generation and transmission	Department of Primary Industries[(a)]
Water	Water, sewerage and dam safety	Department of Sustainability and Environment
Transport	Air, road, sea, rail and inter-modal (cargo distribution centres)	Department of Transport
Communications	Telecommunications (phone, fax, internet, cable, satellites), electronic mass communications and postal services	Department of Innovation, Industry and Regional Development
Health	Hospital, public health and research and development laboratories, private sector pathology laboratories and suppliers of blood products and medical and therapeutic products and services	Department of Human Services
Food Supply	Bulk production, storage and distribution	Department of Primary Industries
Banking and Finance	Banking, insurance and trading exchanges	Department of Innovation, Industry and Regional Development
Police and Emergency Services	Police, fire, ambulance, VICSES and others	Department of Justice Victoria Police
Places of Mass Gathering[(b)]	Commercial centres, cultural, sport and tourism	Department of Planning and Community Development Victoria Police Department of Premier and Cabinet

Note: (a) Machinery of government changes in December 2006 transferred responsibility for policy and oversight of the energy sector from the Department of Infrastructure (now Department of Transport [DOT]) to the Department of Primary Industries (DPI). However, DOT continues to manage DPI's obligations under Part 6 of the Act for the energy sector, under a formal agreement between the two departments.
(b) While not matching the definition of critical infrastructure, places of mass gathering are vulnerable to the same threats. The risk management considerations for places of mass gathering are based on the protection of people rather than on the protection of physical assets.

Source: Department of Premier and Cabinet, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007 and information provided by audited agencies.

The CIP framework provides for the establishment of SCNs for each of the nine critical infrastructure sectors, to bring together state and local government representatives and owners/operators of critical infrastructure to consider relevant security, emergency management and business continuity policies and practices. Each SCN is chaired and administered by the designated lead department.

Under Part 6 of the Act, there is no equivalent structure to drive coordination of activities and communication across, or within, government for declared essential services. For the purposes of managing their essential services responsibilities under Part 6 of the Act, we found that in practice, relevant departments have adopted the same industry sectors that apply under the CIP framework.

We found that the characteristics of the industry sectors have affected the progress made in implementing practices set out under the CIP framework. For example, the health sector is diverse with a large number of operators. As a result, collaboration across the sector is difficult. On the other hand, the water sector is homogeneous and has a history of emergency management planning, systems and processes given the regulatory environment in which it operates. As a result, the activities of its SCN are more advanced and have included initiatives to identify interdependencies with other sectors and presentations by guest speakers to the SCN on a number of security and critical infrastructure protection topics.

The operational maturity of the SCNs varies significantly across the nine sectors and consequently, the governance structure is not fully operational:

- For two industry sectors, transport and water, the SCN is well developed, has met regularly and has made progress in addressing its sector's preparedness to respond. The water sector formed its SCN prior to the development of the CIP framework because it was already collaborating in a Threat Assessment for Water Group. The transport sector was an early adopter with its lead department, the Department of Transport (DOT) playing a major role in developing the CIP framework.
- For the police and emergency services sector, work on security, emergency management and business continuity occurred for some time under the auspices of the Emergency Services Organisations Business Continuity Planning Forum. These activities were taken up by the Police and Emergency Services SCN in May 2007. The owners/operators of critical infrastructure in the sector, Victoria Police and the Department of Justice (DOJ) have met twice under the SCN format.
- For two other industry sectors, energy and food supply, the SCN is operating but is less developed. For the energy sector a set of emergency and business continuity arrangements already exist that link government and industry. The Department of Primary Industries (DPI) is exploring how to develop a role for the energy SCN that does not duplicate what is already in place. The food supply SCN is focusing on identifying members, developing its charter and becoming organised.
- For the health sector, the Department of Human Services (DHS), has not actively communicated the CIP framework to the sector, believing that the sector would not respond favourably to counter-terrorism initiatives due to its focus on 'all hazards, all agencies' emergency management. DHS advised that the SCN held its first meeting in October 2008.

- For the remaining three industry sectors—banking and finance, communication, and places of mass gatherings—SCNs have yet to be established:
  - In two of these sectors, banking and finance and communication, the Department of Innovation, Industry and Regional Development (DIIRD), the lead department, considers that the SCN structure is inappropriate as its sectors operate in the national, rather than state, arena and that the sectors are covered by national infrastructure protection arrangements in which DIIRD participates. DIIRD raised concerns with the proposed SCN structure and its appropriateness for the banking and finance and communication sectors, during consultation on the development of the CIP framework with DPC. These concerns were not resolved. As a result DIIRD has not established, and does not intend to establish, SCNs for these sectors. There is a need to clarify the requirements for DIIRD in relation to establishing SCNs and its national/state responsibilities.
  - For the places of mass gatherings sector, DPC, the Department of Planning and Community Development (DPCD) and Victoria Police, have joint responsibility for the sector. Victoria Police has developed an information pack for owners/operators to assist their protection planning, and DPC is waiting on feedback from DPCD and Victoria Police on a proposed approach to the sector.

Delays in establishing SCNs, and the lack of clarity about whether SCNs should be established, have affected the ability of the governance arrangements to operate with maximum benefit.

As the agency responsible for developing and coordinating whole-of-government strategy and policy for the CIP framework and administering Part 6 of the Act, DPC should:

- review and resolve whether certain industries should establish SCNs. Evidence provided by DPC from a representative of the banking and finance Infrastructure Assurance Advisory Group (IAAG)—the national equivalent to an SCN—highlighted that an SCN for the sector would be valuable as response and recovery must be explored at the state level and not at national level. The advice stated that there would be strong support from the Victorian members of the banking and finance IAAG for an SCN
- provide guidance to lead departments and SCNs to assist development of terms of reference for SCNs.

Subsequent to the audit conduct phase, DPC wrote to the Commonwealth Government proposing a review of national critical infrastructure protection arrangements to address a number of matters including ‘significant and ongoing concern in many jurisdictions about the delineation of roles of the Commonwealth, State and Territory Governments in the arrangements, particularly in relation to liaison with industry…’.

4.2.3 Central agencies

Department of Premier and Cabinet

DPC is the main agency for coordinating Victoria's counter-terrorism policy and activities with the Commonwealth. DPC's SEU takes on this role and plays a significant role in communicating and coordinating the state's approach with the national approach through its participation in, and membership of, the National Counter-Terrorism Committee (NCTC), the primary body for developing Australia's national counter-terrorism arrangements, and various other related national committees and sub-committees. Victoria was the first jurisdiction to establish a security and emergencies unit and this has now been replicated by all jurisdictions, including at the national level. The SEU also maintains the State Crisis Centre to support government when managing extreme emergencies, including terrorism incidents.

The SEU has the key role in developing and coordinating whole-of-government strategy and policy to ensure a consistent approach across government, for protecting critical infrastructure and essential services from the effects of terrorism. We reviewed the activities of the SEU and found:

- it difficult to distinguish between its role relating to the governance arrangements for protecting essential services and critical infrastructure and the role of the G-SCN-CG. The roles of these two bodies need to be clarified to ensure appropriate involvement of, and consideration of matters at, the G-SCN-CG and to enable clear accountabilities to be established
- a need to improve the quality of record keeping by the SEU relating to the development of the Act and CIP framework, including evidence of rigorous review of information provided by departments, and records of discussions and decision-making.

Victoria Police

Victoria Police's Risk Management Unit within the Counter-Terrorism Coordination Unit was established in 2002 following the release of the Government's *Enhancing Victoria's Domestic Security New measures for the fight against terrorism* policy. The Unit was replaced in 2007 by the CIPU which manages Victoria Police's responsibilities under the Part 6 of the Act and CIP framework.

Under Part 6 of the Act, Victoria Police's responsibilities are to supervise, and be consulted by the relevant department about the timing of exercises to test risk management plans of operators and the manner in which the exercises must be conducted, and to report on those exercises to the relevant department. These responsibilities are vastly different from its responsibilities under the CIP framework, which, according to the *Victorian Framework for Critical Infrastructure Protection from Terrorism* document, include:

- identifying critical infrastructure within Victoria
- assisting in the provision of protective security advice and developing protective security strategies to counter-terrorism
- advising owners/operators of critical infrastructure of relevant threat information, in accordance with existing arrangements
- ensuring protective arrangements are in place to protect essential government services, such as utilities and key facilities
- developing and communicating to owners/operators of critical infrastructure the agreed type of response expected for each level of threat and alert
- assisting owners/operators of critical infrastructure in the development, validation and audit of risk management plans
- ensuring liaison is established and maintained with owners/operators
- ensuring that intelligence is gathered and disseminated to relevant agencies as required
- conducting and participating in training exercises to test risk management plans of owner/operators.

There appears to be no rationale for the different responsibilities under the two components of the state's arrangements for protecting essential services and critical infrastructure from the effects of terrorism. Further comments about how Victoria Police operates under the two sets of arrangements are presented in Part 5 of this report.

4.2.4 Departments

'Relevant' departments

Under Part 6 of the Act, the Premier may designate a 'relevant minister' for an essential service. The Act mandates particular activities to the relevant minister in relation to the essential service, including recommending declaration of essential services, advising operators that their essential services have been 'declared', setting timeframes for preparation of risk management plans by operators, determining intervals for operators to prepare and participate in training exercises, and consulting on the form and content of reports on training exercises.

The relevant minister may delegate part of his or her responsibilities to public servants. In this report, the department that carries the delegation from the relevant minister is referred to as the 'relevant department'.

‘Lead’ departments

Under the CIP framework, ‘lead’ departments have key roles and responsibilities that support the protection of critical infrastructure. The *Victorian Framework for Critical Infrastructure Protection From Terrorism* document published in April 2007 sets out specific roles and responsibilities for the six lead departments audited. The specific roles and responsibilities according to the 2007 document are set out in Appendix B of this report.

Given that the functions of lead departments under the CIP framework are largely the same regardless of their sectors, we expected that their documented roles and responsibilities would be similar. However, as Appendix B shows, there are only a few roles in common across the departments—to chair their industry sector SCN and to attend their sector’s national industry-related group Infrastructure Assurance Advisory Group (IAAG). Their other roles vary substantially, although further analysis indicates greater similarity that is not immediately evident. The inconsistent statement of roles and responsibilities has led to confusion amongst departments. In practice, we found that agencies undertake activities that differ from those identified in the CIP framework document. It would be beneficial if the statements of roles and responsibilities were re-cast to provide greater clarity to departments and industry.

Positively, and, over and above their requirements under the CIP framework, several Victorian departments have established emergency management units to coordinate their departmental activities.

4.3 Inter-agency risks

Managing risk is an important component of public sector governance. When departments work across their traditional boundaries in a joined-up capacity, it is important that the risks and opportunities with this arrangement are identified and managed. Failure to appropriately manage these can impact on the development and implementation of policy, service delivery and the achievement of milestones and budget.

The requirement to manage inter-agency risks has been identified in the Department of Treasury and Finance’s *Victorian Government Risk Management Framework,* which recognises the need for agencies to identify and communicate risks where they may impact on other agencies and/or the state.

The importance of managing inter-agency risks was also examined in our 2007 performance audit report *Managing Risk Across the Public Sector* and the 2008 performance audit report *Coordinating Services and Initiatives for Aboriginal People*.

Inter-agency risks are those risks, affecting the operations of one or more agencies, which impact on the service delivery of other agencies. From a joined-up perspective, common risks include:

- if goals for the initiative are not shared or clearly defined, parties may work to different goals, and the outcomes are unlikely to be achieved
- if an agency fails to communicate vital information to another agency to enable it to reliably undertake the activity
- if sufficient and appropriate resources are unavailable (including skilled people), the objectives may not be met
- if the leadership is not clear, this could contribute to the initiative floundering and not achieving its objectives
- if roles and responsibilities are unclear, accountability for success or failure cannot be established.

The key point is that risk management planning processes should take into account an awareness of the impact of risks and strategies on other areas across government and include communication of potential impacts through appropriate channels to the appropriate departments and agencies.

Risks that impact on more than one agency and cannot be managed by one agency or at inter-agency level may require central government coordination of policy initiatives and implementation strategies.

We examined the arrangements in place to determine whether agencies involved in implementing Part 6 of the Act and the CIP framework had identified and managed inter-agency risks.

There are a number of forums where senior departmental representatives consider inter-agency issues relating to emergency management and business continuity on a regular basis. However, for essential services and critical infrastructure, there was little evidence available to indicate that inter-agency risks associated with the joined-up arrangements had been identified or managed at the whole-of-government level. Although DPI in relation to food supply, DSE, DOT, and Victoria Police had identified some inter-agency risks relating to essential services and critical infrastructure there remains significant room for improvement.

4.4 Communication and consultation

We examined the arrangements in place to determine whether meaningful communication and consultation had occurred across government agencies and with operators of declared essential services and owners/operators of critical infrastructure.

4.4.1 National level

At a national level DPC and Victoria Police participate in, and are members of, the NCTC. Both agencies also regularly participate in meetings for several national committees and sub-committees.

One of the stated objectives of the NCTC is to build nationwide capability. Our discussions at the national level revealed that Victoria has been an important contributor in the national arena and provided leadership. For example:

- the SEU has been a strong contributor to the capability development of state crisis centres in Queensland, South Australia, Tasmania, the ACT, Northern Territory and, to a lesser extent, New South Wales
- a SEU representative was the NCTC Crisis Centre Capability Adviser for over four years and during this term led a range of capability development activities including the crisis centre inter-communications system, the crisis centre training framework, the development of principles for teleconferences, incident logs and situation reports as well as umpiring a number of exercises.

Critical infrastructure protection networks

Under the *Critical Infrastructure Protection National Strategy* a trusted information sharing network made up of nine different business sector groups, called Infrastructure Assurance Advisory Groups (IAAG), has been created. The nine national critical infrastructure sectors include banking and finance, communications, emergency services, energy, food chain, health, icons and public gatherings, transport, and water services. These groups are primarily trusted information sharing networks. The IAAGs are overseen by the Critical Infrastructure Advisory Council.

The Victorian Security and Continuity Network structure mirrors the national critical infrastructure protection structure with linkages between the Victorian structure and the national structure at industry and government levels. Under the CIP framework Victoria Police and lead departments are required to attend relevant IAAGs.

We found that:

- Victoria Police and five lead departments—DIIRD, DOJ, DPI, DSE and DOT—attend meetings of their respective IAAGs
- DHS is not invited to attend IAAG meetings for its sector as the IAAG does not have jurisdictional representation.

4.4.2 Whole-of-Victorian-Government level

On counter-terrorism and critical infrastructure protection issues the CGRC and G-SCN-CG provide mechanisms for communicating across government agencies. We found:

- All agencies audited attended CGRC and G-SCN-CG meetings regularly.
- DOT is an active participant in each of the state level forums. A review of the CGRC minutes showed that DOT is the better practice agency in raising issues/updating the CGRC on critical infrastructure protection issues for the two sectors it manages.

- With the release of the CIP framework the G-SCN-CG discussed the development of a communication strategy and establishment of a communications working group. However, the communications working group was not established and the communication strategy was not developed. At the June 2008 meeting of the G-SCN-CG it was agreed that the communication strategy would be removed from the action list until further need was identified, and that the G-SCN-CG terms of reference would be updated leading to the formation of a three to five year strategic plan.
- A whole-of-government website outlining the Victorian security and whole-of-government arrangements with links to authoritative security and emergency management sources, planned in 2006, has not been developed.

4.4.3 Agency level

Protecting critical infrastructure requires the timely exchange of accurate and relevant information in a secure environment. In developing the CIP framework, DPC consulted with all lead departments and Victoria Police.

There is active inter-government communication between some agencies we audited. Lead departments that are relatively well advanced in developing their terrorism response arrangements have been consulted by others, whose arrangements are less advanced. DOT, DPI and DSE were particularly noted as consulting actively. Apart from attending the CGRC and the G-SCN-CG, DIIRD does not interact with DPC, Victoria Police or other government departments in relation to preparedness to respond to terrorism incidents, because of the position it has taken to its national/state responsibilities.

DPC has encouraged appropriate officers to seek security clearances and relevant senior committees have agreed that clearances should be sought by specific classes of officers to enable them to receive classified information. A Whole-of-Victorian-Government policy, advising on the appropriate measures for security classified information, was also promulgated by letter to departmental secretaries in February 2008. Despite this, officers in some departments have not sought these necessary clearances.

While recognising the need for security of information, lead departments need access to information that will help them to encourage owners/operators to protect critical infrastructure from the effects of terrorism incidents.

The arrangements for sharing and safe storage of security-classified information, such as lists of critical infrastructure, need to be addressed so agencies can access information that impacts their sectors. For example, the ability of lead departments to consult and communicate with industry through the SCNs is diminished when departments are not aware of the critical infrastructure listed on the critical infrastructure register for their sector and therefore, the owners/operators of that infrastructure. There is a need for representatives of lead departments to obtain necessary security clearances so that appropriate officers can access information relevant to their sectors.

4.4.4 Industry level—SCNs

SCNs provide the means for communicating with owners/operators of critical infrastructure. In practice, they also provide a means for communicating with operators of declared essential services. The SCNs of only two industry sectors, transport and water, have been established for some time compared with the others and are relatively mature. A range of other arrangements operate in some sectors providing for communication between government and owners/operators in relation to emergency management arrangements and business continuity. We are unable to determine whether such arrangements adequately focus on preparing essential services and critical infrastructure to respond to terrorism incidents.

4.5 Performance monitoring

Performance monitoring is an important part of any program or activity, and is used to measure progress against goals. It:

- enables agencies to assess whether their stated objectives have been achieved
- drives performance improvement
- underpins accountability.

As well as monitoring performance of individual agencies and programs, it is important that joined-up activities are also monitored to assess whether inter-agency actions are achieving their intended results.

A system to monitor performance of the state's arrangements for protecting essential services and critical infrastructure from the effects of terrorism incidents should assess:

- the extent to which agencies are fulfilling their obligations under Part 6 of the Act and CIP framework, e.g., percentage of declared essential services and critical infrastructure that have conducted an annual exercise that tests their risk management plans
- the effectiveness of training exercises in testing the preparedness of operators of essential services and owners/operators of critical infrastructure.

As the agency responsible for coordinating the state's counter-terrorism policy, including Whole-of-Victorian-Government policy for critical infrastructure protection, and given the Premier's responsibility for administering *the Terrorism (Community Protection) Act 2003*, DPC has a central role in supporting the effective operation of the arrangements. In this context, it is important that DPC has in place effective arrangements to measure and monitor its own performance, as well as that of the system. Such information enables reporting to government on performance and enables timely corrective action to address emerging issues and to introduce system improvements.

We found:

- Training exercises are used as a means of testing effectiveness of the arrangements. Formal debriefs were conducted and reports prepared for the sample of exercises reviewed by audit. In most instances the outcomes of major exercises have been reported to CGRC and SECC.
- Since its creation in November 2002, several memos outlining the intended program of the SEU have been forwarded to and agreed by the Secretary of the Department of Premier and Cabinet. Prior to the approval of a Business and Expenditure Plan in December 2006, the SEU did not have a formal business plan. There is scope for improvement in the plan: it lacks clearly defined objectives for the unit aligned with its role in administering Part 6 of the Act and under the CIP framework, key outcomes and milestones against each objective, and outcome measures and targets linked to the objectives. A business plan for 2007–08 was not prepared.
- There is no framework for measuring and monitoring performance of the joined-up arrangements.

In the absence of an overarching performance monitoring framework for the implementation of Part 6 of the Act and the CIP framework, the assessment of progress and success relies on departmental performance monitoring systems. Although three agencies—DSE, DOT and Victoria Police—had limited performance monitoring measures in place these were not sufficient to capture joined-up progress. Departmental performance monitoring systems also need development to enable assessment of departmental performance in implementing the requirements of the Act and the CIP framework.

4.6 Conclusion

Victoria was the first Australian jurisdiction to develop arrangements for protecting essential services from the effects of terrorism, including at the national level. Victoria has played a significant part in developing capability for protecting essential services and critical infrastructure nationally and in other states, in particular the capability development of crisis centres of other states and territories.

The establishment of a governance structure comprising the Security and Emergencies Committee of Cabinet, the Central Government Response Committee, Government Security and Continuity Network Coordination Group (G-SCN-CG) and Security Continuity Networks (SCNs) to underpin the arrangements for protecting essential services and critical infrastructure is a positive initiative. However, the governance arrangements are not entirely effective:

- The co-existence of Part 6 of the Act for essential services and the CIP framework for critical infrastructure, is confusing to agencies, and hinders coordination.
- SCNs are not fully operational, with varying levels of progress. Two of the nine are operating well, One other has recently converted to the SCN format after operating for some time under other arrangements. Two are in the early stages of operation. Another held its first meeting in October 2008. The other three have not been established. Timeframes for implementation of the CIP framework have not been set.
- The effectiveness of the G-SCN-CG has been reduced by the delayed development of the SCNs and the co-chairing arrangements between DPC and Victoria Police. The requirement under the arrangements for the G-SCN-CG to focus on the CIP framework rather than both critical infrastructure and essential services has limited its potential effectiveness.
- Respective roles and responsibilities of agencies involved are unclear, particularly under the CIP framework.
- Efforts to identify and mitigate inter-agency risks associated with joined-up arrangements for managing the framework were not evident.
- An adequate performance measurement and monitoring framework has not been developed.

As a result, levels of preparedness of owners/operators of critical infrastructure and operators of declared essential services to respond to terrorism incidents are at different levels of development across sectors, and are difficult to measure.

It is clear from the government's policy document *Enhancing Victoria's Domestic Security: New measures for the fight against terrorism* that the Department of Premier and Cabinet has responsibility to coordinate Victoria's major incident management, including for counter-terrorism policy and planning. While responsibility for oversight of operators of declared essential services in specific sectors rests with the relevant minister and department, DPC should exercise firmer leadership in administering Part 6 of the Act and implementation of the CIP framework and remove barriers to their effective implementation.

Since the emergence of national arrangements, subsequent to introduction of the 2003 Victorian legislation, and given the issues identified during the audit, it is timely to review the arrangements for protecting the state's essential services and critical infrastructure. Such a review should aim to reduce the complexity of the state's arrangements and streamline practices, consistent with maintaining regulation and coordination to mitigate risks specific to our highly privatised service delivery environment.

DPC advised it intends to examine Victoria's critical infrastructure protection arrangements including Part 6 of the Act and the CIP framework to assess their effectiveness and appropriateness for the near to medium term.

Recommendations

The Department of Premier and Cabinet should:

4.1 establish clear oversight and coordination of the arrangements for both Part 6 of the *Terrorism (Community Protection) Act 2003* and the CIP framework by an appropriate body, such as the Government Security and Continuity Network Coordination Group with expanded responsibilities

4.2 lead the development of a performance management framework for measuring, monitoring and reporting on the implementation of Part 6 of the Act and the CIP framework. The framework should include key indicators, targets and reporting arrangements for assessing the extent to which departments, agencies and industry have fulfilled their obligations, as well as measures for monitoring achievement of joint objectives

4.3 clarify the roles and responsibilities of departments and agencies under Part 6 of the Act and CIP framework to reduce confusion and gaps

4.4 provide definitive guidance on identifying essential services for declaration to better inform relevant departments in discharging their responsibilities under Part 6 of the Act

4.5 identify risks arising from the joined-up nature of the approach to protecting essential services and critical infrastructure, and to assist departments and agencies to develop associated risk management arrangements at the whole-of-government level

4.6 clarify the requirements in relation to establishing Security and Continuity Networks in designated sectors, so that there is a shared understanding of those requirements.

4.7 Representatives of lead departments should obtain necessary security clearances so appropriate officers can access information relevant to their sectors.

5 Compliance

At a glance

Background

Part 6 of the *Terrorism (Community Protection) Act 2003* (the Act) mandates the involvement of operators of essential services in planning for the protection of those essential services against the effects of terrorist acts, responding to and recovering from an attack and the continued safe operation of the service in the event of an attack. It also establishes practices with which operators and relevant departments must comply.

The *Victorian Framework for Critical Infrastructure Protection from Terrorism* (CIP framework) sets out the guiding principles and coordination arrangements for government and industry to jointly develop strategies for protecting Victoria's critical infrastructure. It also encourages industry to take up practices consistent with those required of operators of essential services.

Key findings

- Essential services in the three most significant areas of essential services—energy, transport and water— have been 'declared' under the Act and alternative arrangements in place for the police and emergency services sector are considered reasonable. As departments in the remaining sectors have yet to consider whether such declarations are necessary, we were unable to gain assurance whether all essential services have been declared.
- The three departments that have 'declared' essential services have provided oversight and assistance to operators of those services to assess and prioritise risks in their sectors and develop risk management plans.
- Victoria Police has established a register of the state's critical infrastructure. Despite Victoria Police providing listings to lead departments in 2004, three departments audited were not aware of critical infrastructure listed on the critical infrastructure register for their sectors. This compromises their ability to work with owners/operators to meet requirements under the CIP framework.

At a glance – *continued*

Key recommendations

DPC, in consultation with Victoria Police, should develop clear guidance to distinguish between declared essential services and critical infrastructure to assist departments, Victoria Police and industry in implementing Part 6 of the Act and the CIP framework more effectively. **(Recommendation 5.1)**

DPC should provide clear guidance on terms such as ‘audit’, ‘auditor’ and ‘adequacy of the exercise’ to assist departments, Victoria Police and industry to implement requirements more reliably. **(Recommendation 5.2)**

DPC and Victoria Police, in consultation with departments, should standardise reporting on training exercises conducted under Part 6 of the Act and the CIP framework to promote greater consistency and to enable better identification of lessons learned and continuous improvement. **(Recommendation 5.3)**

Reports on the training exercises should be retained in an appropriately secured central repository so that consolidated results of the exercises can be drawn together effectively. **(Recommendation 5.4)**

5.1 Introduction

Part 6 of the *Terrorism (Community Protection) Act 2003* (the Act) mandates operators of declared essential services to be involved in planning for the protection of those essential services, for responding to and recovering from an attack and the continued safe operation of the service in the event of an attack. For the purposes of the Act, essential services are transport, fuel (including gas), light, power, water, sewerage and a service declared to be an essential service by the Governor-in-Council under the Act.

The *Victorian Framework for Critical Infrastructure Protection from Terrorism* (CIP framework) sets out the guiding principles and coordination arrangements for government and industry to jointly develop strategies for protecting Victoria's critical infrastructure. Critical infrastructure are physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of Victoria and its community.

The Act sets out requirements with which operators and relevant departments are required to comply. The requirements for operators include development of risk management plans, annual audit of those plans and the conduct of training exercises to test those plans at least annually. The CIP framework encourages owners/operators to take up the same practices required of operators of essential services, and sets out structures to assist lead departments and industry to work together.

5.2 Identifying essential services and critical infrastructure

Awareness of the declared essential services and critical infrastructure in their areas of responsibility is fundamental to effective agency monitoring of compliance. Before determining the extent of compliance with the requirements of the Act and recommended practices under the CIP framework, we examined whether the six departments and Victoria Police, had identified the essential services and critical infrastructure in the nine industry sectors for which they were responsible.

5.2.1 Identifying essential services

The Act sets out the broad types of essential services to which it applies, e.g., transport, power and water. It also provides for other types of services to be declared as essential services on the recommendation of a relevant minister. The Act does not establish criteria for identifying specific infrastructure sites or services to be declared as essential services. This has affected the ability of departments to identify and, therefore, declare essential services.

However, two departments were proactive in developing the means to identify essential services.

The Department of Sustainability and Environment (DSE) used a consultative process involving other departments, an industry association, Victoria Police and its Security and Continuity Network to develop a common understanding in meeting the requirements under the Act and to provide guidance on definition, terms and requirements. DSE declared its essential services in the water sector in mid-2007. DSE did not declare its essential services earlier because it considered the operators:

- had relatively good emergency management plans, systems and processes in place along with appropriate regulatory and compliance mechanisms, when compared with other essential services
- are publicly owned and therefore required less regulation in comparison with other essential services, which have significant private sector involvement.

However, following amendments to the Act in June 2006, which included more stringent compliance measures, DSE considered it prudent to declare the essential services under the Act.

The Department of Transport (DOT) undertook reviews in 2003 and 2005 to assist identification of the services in the energy and transport energy sectors. It has also acted to establish criteria, given the absence of criteria in the Act, to identify specific infrastructure sites or services within the broad essential service types.

To determine whether services should be declared essential DOT considers:

- whether the service is critical
- ASIO threat assessment indicating a higher level of potential risk
- an assessment of the potential impact on the essential service and its interdependencies with other essential services and critical infrastructure.

DOT declared essential services in the transport and energy sectors in 2004 and 2006.

At the time of the audit, 39 essential services have been declared in the energy, transport, and water sectors managed by these three departments.

For the police and emergency services sector, essential services have not been declared by DOJ under Part 6 of the Act because business continuity, security and emergency management are already part of the responsibility of the agencies within that sector, and government. These agencies, which include Victoria Police and the ambulance and fire services, have reporting responsibilities to the Victorian Emergency Management Council and the CGRC. Testing of emergency services is undertaken as part of normal operations within the sector. Formal arrangements and representation at state-level forums already exist under the Victorian emergency management arrangements and activities for this sector. The department's position that declaration of essential services is not required for this sector is considered reasonable.

The remaining three departments audited—the Department of Human Services (DHS), and the Department of Innovation, Industry and Regional Development (DIIRD) and the Department of Primary Industries (DPI) in respect of the food supply sector—have not declared any essential services in their industry sectors. These departments do not have processes for identifying essential services for declaration. DPI is in the process of reviewing the food supply sector to identify the relevant essential services, if any.

As departments in these sectors have yet to consider whether such declarations are necessary, we were unable to gain assurance whether all essential services have been declared.

5.2.2 Identifying critical infrastructure

Under the *National Counter-Terrorism Plan* and *National Counter-Terrorism Handbook*, state and territory governments have been assigned responsibilities to identify critical infrastructure, in their jurisdictions, and to put in place systems and procedures to manage the risk to that critical infrastructure. Under the CIP framework, Victoria Police is the agency responsible for identifying and prioritising Victoria's critical infrastructure.

Victoria Police has established a register of critical infrastructure and there are currently 256 listings on the register. However, there was little evidence of consultation between Victoria Police and lead departments about which infrastructure should be on the register. In this regard DHS, DIIRD and DOJ advised that they have not been consulted.

Victoria Police provided a listing of the critical infrastructure for individual sectors to the individual lead departments in 2004 via the CGRC. Despite this three departments audited—DHS, DIIRD and DOJ—were not aware of critical infrastructure listed on the critical infrastructure register for their sectors. This inhibits their ability to work with owners/operators to implement recommended practices.

There is no process for lead departments to access information in the critical infrastructure register. Despite the security issues, there were examples where lead departments have been proactive in working with Victoria Police to determine the critical infrastructure in their sectors. DPI is conducting a review to identify critical infrastructure within the food supply sector and has been granted access to the register by Victoria Police. DHS has also recently requested to view the register and is making arrangements for appropriate storage of this information.

DHS, DIIRD and DOJ do not have processes for identifying critical infrastructure in their sectors for a range of reasons:

- DIIRD, considers that jurisdiction over the two industry sectors concerned rests at the national level.

- DHS and DOJ advised that they work within the 'all hazards, all agencies' approach to emergency management. DHS has not actively communicated the CIP framework to its industry sector, believing that the sector would not respond favourably to counter-terrorism initiatives due to the sector's focus on 'all hazards, all agencies' emergency management. DOJ advised that the CIP framework interfaces with the 'all hazards, all agencies' arrangements.

These three lead departments are therefore not yet in a position to encourage owners/operators in their industry sectors to take up recommended practices aimed at protecting critical infrastructure from the effects of terrorism incidents.

5.2.3 Distinguishing essential services from critical infrastructure

At the time of the audit there were 39 essential services declared under the Act and 256 critical infrastructure sites registered across Victoria. In 19 cases the same site was both a declared essential service and included on the critical infrastructure register. This creates confusion, given that the requirements of the Act are mandatory while recommended practices under the CIP framework are not.

Victoria Police plans to review the critical infrastructure register to determine whether all sites listed should be registered. Clear guidance to distinguish between 'declared essential services' and 'critical infrastructure' would assist Victoria Police in this review, go some way to eliminating the overlap, and assist agencies and industry in implementing Part 6 of the Act and the CIP framework.

5.3 Risk management

The risk management plan specified in Part 6 of the Act, which may form part of any other risk management plan prepared by the owner for the essential service must contain, amongst other things:

- an assessment of the risks to the essential service/critical infrastructure of terrorist acts
- a plan of the measures to be undertaken to prevent or reduce the risk including ensuring the physical security of key infrastructure
- a plan for the measures to be taken in the event of a terrorist act including:
  - the procedures for response to the terrorist act
  - the procedures for recovery of the essential service/critical infrastructure from the terrorist act
  - the procedures to provide for the continued safe operation of the essential service/critical infrastructure
- details of the positions of the persons responsible for the operation of the risk management plan in the event of a terrorist act

- details of the measures to be taken to protect the essential service/critical infrastructure in the event of a terrorist act on another essential service on which the essential service/critical infrastructure is dependent
- details of the coordination of the risk management plan with any relevant municipal emergency management plan prepared under the *Emergency Management Act 1986*
- details of the training to be provided to staff in relation to the procedures to be followed to prevent or respond to terrorist acts.

The risk management plan must comply with any prescribed standard. The relevant standard for Victoria is the *Australian and New Zealand Risk Management Standard AS/NZS 4360:2004*.

The CIP framework recommends that owners/operators of critical infrastructure also adopt these risk management arrangements.

To gain a common understanding in meeting the requirements under the Act and to provide guidance on definition, terms and requirements:

- DSE conducted three workshops with all corporations in the water sector and relevant stakeholders in 2007, and has developed guidelines to assist its declared essential services to conduct and assess exercises and to assess risk management plans.
- DOT prepared the *Risk Management Kit for Terrorism* (the Kit) which was distributed to operators of declared essential services in the energy and transport sectors. The Kit is an integrated resource for the energy and transport sectors. We found the Kit is concise and easy to understand, targeted and complementary to the CIP framework and requirements of Part 6 of the Act.

5.3.1 Assessing and prioritising risks

Relevant and lead departments

While not responsible for developing the risk management plans, consistent with Victoria's approach to protecting essential services and critical infrastructure from terrorist acts, relevant and lead departments are involved in providing support to their industry sectors.

DPI for its energy sector, DSE and DOT have provided oversight and assistance to operators of declared essential services in the energy, water and transport sectors to assess and prioritise risks and develop risk management plans. Other departments have played no role in assessing and prioritising risks under Part 6 of the Act because there are no declared essential services in their sectors at this time.

DSE has provided oversight for its sector. The operators in the water sector have relatively well established and tested emergency management plans, systems and processes in place based on an 'all hazards, all agencies' approach, along with regulatory and compliance mechanisms. In this case, the department provided advice and guidance on the use of the *Security Vulnerability Risk Assessment Guideline* (SV RAG) assessment methodology as the basis for identifying and assessing asset vulnerability and measures/actions to protect the asset, in 2003 and 2008. The information was coordinated by DSE and forwarded to Victoria Police for consideration and further assessment to assist identification of critical infrastructure for the sector.

DPI for its energy sector and DOT have provided input to operators of essential services in the development of risk management plans. While DOT does not aggregate or prioritise risks identified in risk management plans, it has identified strategic risks relating to the energy and transport sectors at the very broad level in the *2007–08 Security and Emergency Management Division Business Plan* and undertook a review of security risk management in the two sectors, energy and transport to assist identification of several areas of priority.

The Commonwealth Government developed Critical Infrastructure Protection Modelling and Analysis (CIPMA) to examine the relationships and dependencies between critical infrastructure systems. At present four industry sectors are engaged in the CIPMA program: banking and finance, communications, energy and water.

We found that DPI for its energy sector, DSE and DOT are actively involved in the CIPMA work and have arranged several meetings between the operators, national bodies, the CIPMA team and the Commonwealth Attorney General's Department as part of the stakeholder engagement process. These departments also successfully conducted a trial earthquake scenario, modelling the impacts across electricity transmission, gas transmission, water supply pipe lines, dams, bridges and roads, power generation, buildings and people, and direct impacts on supply of local labour and on emergency recovery processes in the region.

DOT has also established a project to improve the security of a key precinct encompassing Southern Cross Station and facilities around the station. While the project is in its initial stages, DOT has established a committee to coordinate the security and emergency management arrangements across the precinct. The department intends to develop a precinct-wide security and incident response framework focusing on counter-terrorism for a number of precincts.

DIIRD, with responsibility for the banking and finance and communications sectors, is aware of the CIPMA methodology. While the department has had some involvement with CIPMA, there has been limited analysis undertaken.

Of the six lead departments audited only DPI for its energy sector, DSE and DOT have:

- conducted planning
- developed protocols that define the roles and responsibilities of owners/operators and the methods used to interact and share information related to protection of infrastructure
- identified approaches to assess risks.

The remaining lead departments have played little part in assessing and prioritising risks for their sectors under the CIP framework.

Victoria Police

Victoria Police is responsible for assisting owners/operators of critical infrastructure in the development and validation of risk management plans, under the CIP framework. In early 2003, Victoria Police circulated interim protocols to assess threat levels associated with critical infrastructure to owners/operators. Following this, the owners/operators were periodically briefed on their responsibilities.

In January 2007 Victoria Police developed a *Critical Infrastructure Protection Policy* detailing its responsibilities in relation to protection of critical infrastructure. However, we found that the policy:

- expired in January 2008 and is being reviewed
- did not include all Victoria Police's responsibilities outlined in the CIP framework. In particular it does not include Victoria Police's responsibilities to:
  - develop, and communicate with owners/operators of critical infrastructure about, the agreed type of response expected for each level of threat and alert
  - assist owner/operators of critical infrastructure in the development, validation and audit of their risk management plans.

Victoria Police has also prepared a guide, for owners/operators of critical infrastructure, which includes information on the expected level of action for each alert level. The guide is being reviewed because Victoria Police believes it is out of date.

Victoria Police prioritises its activities by:

- focusing the Critical Infrastructure Protection Unit (CIPU) on assisting owners/operators of 'vital' critical infrastructure, that is, where the associated services are considered to be 'integral to the Victorian community and where alternative services cannot be provided within the state'

- delegating the task of inspecting the remaining critical infrastructure sites to local police. Under the Victoria Police *Critical Infrastructure Protection Policy*, local emergency management inspectors are responsible for maintaining contact with owners/operators of registered critical infrastructure and for liaising about prevention, preparedness and response arrangements. The inspectors are to visit critical infrastructure sites within their region quarterly, and submit contact details and site security information to the CIPU. Victoria Police advised that during 2007–08, not all critical infrastructure sites had been visited quarterly. A review is being conducted by CIPU to determine how many have been visited.

In addition to this regime, Victoria Police undertakes security assessments of critical infrastructure sites, places of mass gatherings and locations conducting or hosting major events. Since 2006, Victoria Police has undertaken security assessments for 32 (12.5 percent) of the 256 critical infrastructure sites on the register. These security assessments are not a requirement under the Act or CIP framework. However, Victoria Police advised that they provide valuable information to owner/operators in assessing their risks. Security assessments have also been undertaken for the FINA World Swimming Championships, MotoGP, Grand Prix and Security Regulated Airports.

5.3.2 Auditing risk management plans

Responsibility for ensuring that risk management plans for declared essential services are audited annually and updated to address the outcomes of the audit, rests with operators of those services. Relevant departments may assist the operators in this regard.

In respect to auditing of risk management plans of essential services, of the three departments that have declared essential services:

- as DSE did not declare its essential services until mid-2007, at the time of our audit, the services were still in the first year of their compliance cycle and had not been audited. DSE has agreed to work with the water industry to develop guidance for conducting the annual audit.
- to complement its testing arrangements DOT has engaged a private provider to review selected risk management plans of declared essential services against the requirements of the Act, and to provide a report for each risk management plan reviewed, including suggested improvements. At the time of the audit, the firm had reviewed 11 risk management plans.
- DOT maintains a spreadsheet to record the status of risk management plans, audit certificates and training exercises for services in the energy and transport sectors. We were, however, unable to locate all relevant documentation for a sample of services, to determine whether owner/operators had complied with the requirements under Part 6 of the Act. There were instances of incomplete records from owners/operators for two of the nine cases reviewed.

- for six of the nine files examined we were unable to locate the police report. DOT was not aware of whether the file was incomplete because:
  - a police report had not been completed
  - the document had not been provided to DOT
  - the document had been provided to DOT but not filed.

DOT accepts that it needs to put procedures in place to address the availability of police reports.

Under the CIP framework, Victoria Police is responsible for assisting owners/operators of critical infrastructure in the validation and audit of risk management plans. Victoria Police advised that data was not available to determine what percentage of risk management plans had been audited. However, not all the risk management plans of registered critical infrastructure have been audited annually.

Definitions

Despite either requiring or encouraging annual audits of risk management plans, we found that:

- the term ‘audit’ has not been defined under the Act or the CIP framework
- there is no guidance available to departments or owners/operators of the qualifications required to be an ‘auditor’ of risk management plans.

To facilitate a reliable basis of assurance and consistent practice across industry sectors, clear guidance on these terms should be provided.

5.3.3 Training exercises to test risk management plans

Declared essential services

The Act provides that, at least once in each year, the operator of a declared essential service must:

- prepare a training exercise to test the operation of the risk management plan for the declared essential service
- participate in that training exercise under the supervision of the Chief Commissioner and the relevant minister.

The training exercise must comply with any prescribed standard.

Victoria Police’s responsibilities under Part 6 of the Act are to:

- supervise the training exercise
- report in writing to the Chief Commissioner and the relevant minister on the adequacy of the exercise.

Two of the three departments that had ‘declared’ essential services—DPI for its energy sector and DOT—had regularly conducted training exercises as required under Part 6 of the Act.

We assessed the reports from a selection of training exercises conducted under Part 6 of the Act, for two of the three industry sectors that have declared essential services, namely energy and transport. We found that:

- the term 'adequacy of the exercise' is not defined in the Act. In the absence of a definition, Victoria Police indicates in its exercise reports that an exercise has been conducted. It does not provide an opinion on whether the exercise was adequate to test the plan
- while Victoria Police attends an exercise and writes a report about the conduct of the exercise, it is not required to assess whether the content of the risk management plan is appropriate to mitigate the risk. While reports had been prepared by Victoria Police for the selection of exercises reviewed, the reports did not identify deficiencies in the plans or make recommendations to address them
- exercise reports were consistently prepared by DOT, and by DPI for its energy sector. Since early 2008, DOT has developed and adopted a standardised exercise de-brief report template that is consistent with the prescribed standards for training exercises, to ensure consistency in reporting approach and capture of lessons learned.

For the water sector, we found that DSE and four operators of essential services in the water sector have conducted training exercises to test the risk management plans. DSE has also developed appropriate processes to facilitate compliance with Part 6 of the Act. These include:

- a proposed schedule for training exercises
- risk management plan compliance schedule for 2008–09
- an Exercise Program Planner for all declared essential services
- mapping out of the annual compliance milestones for the industry sector
- mapping out a schedule of the risk management plan exercise approval processes.

Critical infrastructure

Under the CIP framework, Victoria Police is responsible for conducting and participating in exercises to test risk management plans. Not all the risk management plans of registered critical infrastructure have been tested annually. Victoria Police advised that its CIPU does not have the level of resources to ensure that risk management plans for all critical infrastructure are tested annually. CIPU does, however, attend training exercises of which it is advised.

Other training exercises

Because DHS, DIIRD, DOJ and DPI for its food supply sector have not declared essential services, they have played no role in testing risk management plans for their industry sectors under Part 6 of the Act.

Similarly, the four departments have played no role in testing risk management plans for their industry sectors under the CIP framework. However, all agencies audited have participated in training exercises to test emergency response either under Victoria's broader emergency response protocols or national exercises, for example:

- DHS regularly conducts training exercises to test 'emergency response capability'. These tests are primarily focused on testing broad emergency response protocols based on Victoria's 'all hazards, all agencies' approach. Since July 2005, DHS has coordinated 23 emergency management exercises across Melbourne and regional centres. In most instances, each included a major focus on the capability of large health agencies such as hospitals in its industry sector, to respond to large scale critical incidents. In a few instances, the exercises were state-level exercises coordinated by other organisations with a significant medical focus requiring a specific coordination role by DHS.
- The banking and finance Infrastructure Assurance Advisory Group ran a flu pandemic exercise in early 2008 and DIIRD facilitated involvement of a number of Victorian organisations.
- DOT participates in national transport security discussion exercises through the national intergovernmental Transport Security Working Group and the national Transport IAAG.
- DPI for its energy sector regularly consults with National Electricity Market Management Company and VENCorp on emergency management matters and is a member of the National Gas Emergency Response Advisory Committee and the National Oil Supplies Emergency Committee. All these organisations and committees run emergency exercises that involve DPI and the industry.
- DOJ and the police and emergency services sector is heavily involved in exercises and training that are either part of or directly related to protection against terrorism. The sector has involvement in emergency management exercises including National Counter Terrorism Committee (NCTC) counter-terrorism exercises, and emergency services organisations are regularly involved in emergency management and associated exercises with owners/operators of critical infrastructure and local, state and Commonwealth governments.

Since 2005, DPC, DOT, DPI for energy, and a range of other departments and agencies have conducted an ongoing exercise program, known as Project Trident, involving both industry and agencies addressing major security incidents in railway, port and energy infrastructure.

Victorian departments periodically participate in NCTC multi-jurisdictional exercises and major whole-of-Victorian-government inter-agency exercises to test counter-terrorism arrangements and whole-of-government emergency management arrangements. Since 2002, six exercises have been undertaken, coordinated by three exercise directors who are the state's NCTC members and the Executive Director of the relevant Commonwealth agency. Exercise development was led by Victoria Police. The exercises also include a number of emergency services agencies, government departments, volunteer organisations and operators of declared essential services and owners/operators of critical infrastructure.

The operations of the State Crisis Centre and secondary crisis centre, both managed by DPC, are also tested periodically either as part of national or state training exercises. Training exercises and an independent assessment of an international expert have found the centre to be effective.

5.3.4 Monitoring and measuring effectiveness and continuous improvement

Review of training exercise reports

Victoria is committed to continuously improving its emergency management arrangements based on reports from training exercises. For example, the 2002 national exercise 'New Dawn' indicated that the Victorian State Crisis Centre arrangements were inadequate and as a result the centre was reconfigured. The NCTC Mercury 04 exercise demonstrated that the interim configuration was effective. Subsequently, the government commissioned and funded the dedicated State Crisis Centre that became operational in 2005.

In 2005 the Australian National Audit Office tabled its report; *Review of the Evaluation Methods and Continuous Improvement Processes for Australia's National Counter-Terrorism Coordination Arrangements*. This report identified a number of key steps to drive continuous improvement:

- effective capture of results
- analysis of the lessons learned so that the captured information is easily used by decision-makers and allows for efficiencies in the corrective actions
- clear assignment of responsibility for implementing the required actions
- systematic and coordinated monitoring of the implementation of these actions
- further assessment to ensure the ongoing effectiveness of the arrangements as well as measuring the impact of the introduction of new elements.

We reviewed 20 reports on training exercises, to assess whether they demonstrated an effective emergency response by participants to emergency incidents, including terrorism incidents. Fourteen of the training exercise reports we examined were exercises under Victoria's 'all hazards, all agencies' emergency response framework. The exercise reports varied in format, content and analysis which made it difficult to compare the results of exercises so that the extent to which improvement is occurring was difficult to assess.

In all instances reviewed, where exercise reports captured lessons learned, the information was held separately by agencies. Victoria Police maintains a 'lessons learned' database in which it records the outcomes of NCTC coordinated exercises. Departments retain reports in their individual departmental files.

The lack of a central repository for exercise reports makes collective analysis of outcomes difficult. We note that in July 2008 an Emergency Management Exercise Group was established within the Office of the Emergency Services Commissioner (DOJ), to more effectively coordinate 'all hazards, all agencies' emergency exercises, to maintain a database of exercises and lessons learnt and to ensure issues are addressed in subsequent exercises.

Establishing an appropriately secured central repository for retaining the results of all exercises, whether conducted under the NCTC, the state's 'all hazards, all agencies' emergency management arrangements, Part 6 of the Act or the CIP framework would enable lessons learned to be drawn together effectively

For the exercises we examined, a systemic process for continuous improvement was not evident, at either the whole of government or agency level, and we saw no evidence of strategic analysis of recommendations. Consequently, it is not apparent that reports are driving continuous improvement.

While it was not possible to verify a process of continuous improvement, all agencies that had conducted regular training exercises under either the 'all hazards, all agencies' framework of emergency response or under Part 6 of the Act, placed a high priority on continuous improvement. This was clearly evident for DOT, which had conducted regular training exercises under Part 6 of the Act. The department had recently reached a level of 'maturity' to enable it to move from a basic compliance monitoring role, to a more proactive role in providing advice and guidance to operators for the purposes of continuous improvement.

5.4 Conclusion

Three departments audited have declared essential services under the *Terrorism (Community Protection) Act 2003* (the Act). The three departments that have declared essential services—DPI for its energy sector, DSE and DOT—are working to ensure operators of those essential services are operating in compliance with the Act. These departments have taken a proactive approach with their industry sectors, providing support and guidance to operators. We note that the energy, transport and water sectors managed by these three departments are the most significant industry sectors in terms of providing for continuity of operation of the state and its ability to recover from a terrorist incident. Alternative arrangements in place for the police and emergency services sector to prepare to respond to emergency incidents are considered reasonable.

While all departments operate under the state's 'all hazards, all agency' approach to emergency management, there is a need for the departments that have yet to declare essential services in the remaining sectors to consider whether such declarations are necessary. In the absence of evidence of this consideration, we could not gain assurance that all essential services have been declared.

Three lead departments are not aware of the critical infrastructure listed on the critical infrastructure register for their industry sectors and therefore are inhibited in their ability to work with owners/operators to encourage them to take up the recommended practices identified in the *Victorian Framework for Critical Infrastructure Protection from Terrorism* (the CIP framework).

While there is a requirement for risk management plans of declared essential services to be audited annually and annual audits of risk management plans for critical infrastructure are encouraged, what constitutes an audit has not been defined. Similarly there is no guidance on the qualifications required of an auditor who can audit the plans. To facilitate achievement of appropriate standards and consistency of practice, clear guidance on these matters is needed.

Training exercises are conducted under the Act, the CIP framework and the *Emergency Management Act 1986* and national arrangements to test risk management plans and the ability of agencies and industry to respond to emergency incidents, including terrorist incidents. Apart from a 'lessons learned' database that is maintained by Victoria Police and records the outcomes of all NCTC coordinated exercises, there was little evidence of a systemic capacity to capture information about exercises conducted under Part 6 of the Act and the CIP framework. The lack of a central repository for exercise reports makes collective analysis of outcomes difficult. We saw no evidence of strategic analysis of recommendations and consequently, it is not apparent that reports are driving continuous improvement.

Recommendations

5.1 DPC, in consultation with Victoria Police, should develop clear guidance to distinguish between declared essential services and critical infrastructure to assist departments, Victoria Police and industry in implementing Part 6 of the Act and the CIP framework more effectively.

5.2 DPC should provide clear guidance on terms such as ‘audit’, ‘auditor’ and ‘adequacy of the exercise’ to assist departments, Victoria Police and industry to implement requirements more reliably.

5.3 DPC and Victoria Police, in consultation with departments, should standardise reporting on training exercises conducted under Part 6 of the Act and the CIP framework to promote greater consistency and to enable better identification of lessons learned and continuous improvement.

5.4 Reports on the training exercises should be retained in an appropriately secured central repository so that results of the exercises can be drawn together effectively.

6 Funding

At a glance

Background

Since 2002 the government has implemented a number of short and long-term measures to increase the state's counter-terrorism capability.

Key findings

- Quantifying total expenditure on preparing to respond to terrorism incidents is not possible as all expenditure for this component of counter-terrorism activities is not specifically compiled.
- Since November 2002 the government has allocated around $255 million for all counter-terrorism policies, arrangement and capabilities across the state. All agencies audited, except the Department of Innovation, Industry and Regional Development, have received funding under these initiatives.
- Relevant and lead departments have not received specific funding for their responsibilities under Part 6 of the *Terrorism (Community Protection) Act 2003* or the *Victorian Framework for Critical Infrastructure Protection from Terrorism*.
- Victoria Police received funding for undertaking its responsibilities under Part 6 of the Act. It is not funded for undertaking the additional responsibilities introduced under the CIP framework in 2007.

6.1 Funding of counter-terrorism initiatives

6.1.1 Introduction

Since 2002 the Victorian Government has implemented a number of short and long-term measures to increase the state's counter-terrorism capability.

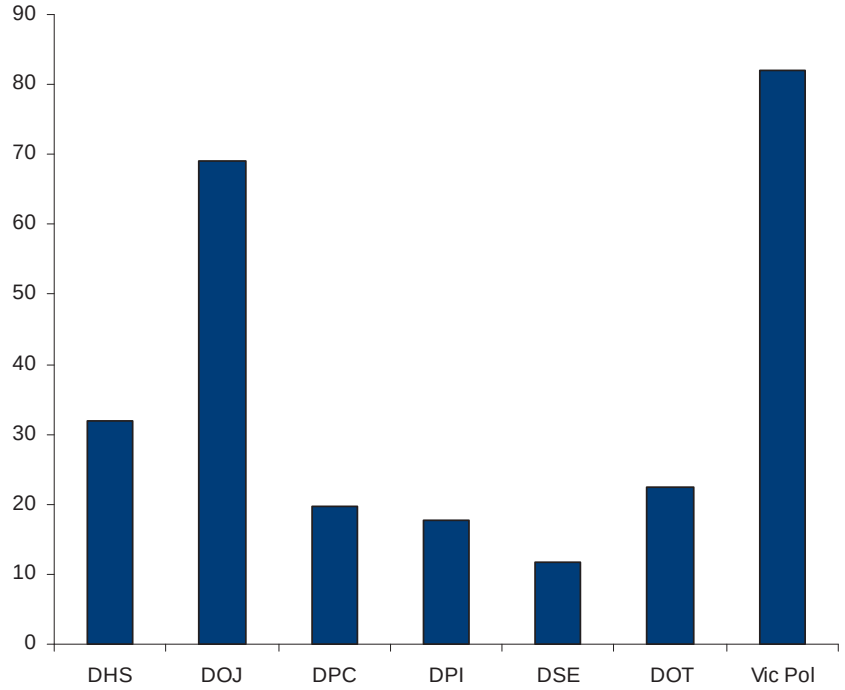
Key measures undertaken include:

- reviewing security at major facilities
- enhancing Victoria's legislative framework to deal with terrorism
- introducing a framework to improve protection of critical infrastructure
- investing significant resources in improving response and investigation capabilities
- playing a significant role with national and other state and territory governments to develop a national counter-terrorism plan
- participating in several major national counter-terrorist exercises involving all relevant state, territory and Commonwealth agencies.

6.1.2 Investment in preparedness to respond to terrorism incidents

Quantifying the state's expenditure on preparing to respond to terrorism incidents is not possible as expenditure is not specifically compiled. Since the release of *Enhancing Victoria's Domestic Security: New measures for the fight against terrorism* in November 2002, the government has allocated around $255 million for all counter-terrorism policies, arrangements and capabilities across the state. Figure 6A shows the funding allocated by agency for the period October 2002 to June 2009.

Figure 6A
Counter-terrorism initiatives: funding allocated, by audited agency
October 2002 to June 2009 ($million)



Source: Selected agencies and Department of Treasury and Finance, *Budget Paper No. 3*, 2002–03 to 2008–09.

Legend:

DHS	Department of Human Services
DOJ	Department of Justice
DPC	Department of Premier and Cabinet
DPI	Department of Primary Industries
DSE	Department of Sustainability and Environment
DOT	Department of Transport
Vic Pol	Victoria Police

As is evident from Figure 6A, Victoria Police has received in excess of $82 million funding for counter-terrorism initiatives. These initiatives have provided additional capability to detect and disrupt terrorist activity, improve coordination of counter-terrorist activities and improve intelligence gathering and investigations systems.

A breakdown of the specific counter-terrorism initiatives funded for the audited agencies is provided in Appendix A.

An advantage of the 'all hazards, all agencies' approach to emergency management is that resources purchased for counter-terrorism can also be used for other emergencies. The government has focused its funding on ensuring police, emergency services and agencies have the capabilities to deal with a wide range of emergencies, including terrorism. As such, the $255 million invested by the Victorian Government in counter-terrorism since 2002 also contributes to the government's broader emergency management capabilities. For example, the State Emergency Service was funded for six lighting trailers to illuminate scenes of terrorist attacks. These lighting trailers provided illumination at the Kerang rail disaster and the Gippsland floods as well as many traffic accidents and other emergencies.

We found that:

- all audited agencies except the Department of Innovation, Industry and Regional Development received some funding for counter-terrorism initiatives during the period
- none of the departments received specific funding for their responsibilities under the *Terrorism (Community Protection) Act 2003* (the Act) or *Victorian Framework for Critical Infrastructure Protection from Terrorism* (CIP framework)
- Victoria Police received funding for undertaking its responsibilities under the Act but was not funded for undertaking additional responsibilities introduced under the CIP framework in 2007, which include assisting owners of critical infrastructure in the development, validation and testing of their risk management plans. The rationale for the different funding approaches was not evident.

As a state with a number of privatised essential services, Victoria has adopted a similar approach to protecting those services as is outlined in the United States *Strategy for Homeland Security* released in 2002. That strategy states that:

> 'A close partnership between the government and private sector is essential to ensuring that existing vulnerabilities to terrorism in our critical infrastructure are identified and eliminated as quickly as possible. The private sector should conduct risk assessments on their holdings and invest in systems to protect key assets. The internalisation of these costs is not only a matter of sound corporate governance and good corporate citizenship but also an essential safeguard of economic assets for shareholders, employees and the nation.'

Through the Act and CIP framework, the responsibility for providing adequate security of declared essential services and critical infrastructure rests with the operators or owners of those facilities. As a result, actions to mitigate identified risks are generally expected to be funded by the owner/operator. We found that the departments have not aggregated or prioritised risks identified in their sectors for the purposes of allocating resources to operators or owners.

6.2 Conclusion

The government has invested around $255 million in counter-terrorism initiatives, since 2002, to protect the community against terrorism including prevention, response and recovery. Victorian Police, emergency services, health services and other government agencies have been provided with new tools to combat terrorism and its consequences.

Because of the nature of terrorism, it is difficult to know when sufficient resources have been provided and it is impractical and very expensive to ever be fully prepared to respond to terrorism incidents. So, preparedness is predicated on the determination of a level of acceptable risk. The level of acceptable risk is a matter of judgment for government, and may change over time.

Appendix A.

Funding counter-terrorism initiatives

Figure A1

Funding allocated for counter-terrorism related initiatives, by agency, by year

Initiative	Year	$m
Department of Human Services		
Recruit extra staff to improve emergency services	2002–03	11.40
Public health laboratory	2004–05	3.47
Trauma Support Program	2004–05	1.40
Hospital negative pressure isolation rooms and refreshed disaster kits	2004–05	5.47
Equipment and training for DHS and ambulance services	2006–07	0.65
Increase emergency response capability	2007–08	9.60
Subtotal		***31.99***
Department of Justice		
Develop training and investigation capacity at the State Coroner's Office	2003–04	1.06
Additional training, equipment and capacity for the Victorian Institute of Forensic Medicine	2003–04	2.67
Protective equipment for Country Fire Authority and Victoria State Emergency Service staff and volunteers	2003–04	3.70
Increase urban search and rescue capability of the Metropolitan Fire and Emergency Services Board	2003–04	20.20
Specialist personnel protective equipment for mass casualties and stand alone mobile lighting towers	2004–05	0.92
Purchase of computerised tomography equipment to assist with mass disaster identification by the Victorian Institute of Forensic Medicine	2004–05	2.15
Grevillea Unit Barwon Prison to create a new 27 bed security unit to house high risk prisoners	2006–07	8.40
Extra judge along with supporting costs such as staff, juries and office space to deal with terrorism and organised crimes	2006–07	5.47
Office of Public Prosecutions additional prosecutorial team to support additional judicial officer	2006–07	2.80
Victorian Legal Aid for defendants charged with organised crime or terrorism matters	2006–07	8.00
Additional staff at Corrections Victoria	2006–07	12.00

Figure A1 – *continued*

Funding allocated for counter-terrorism related initiatives, by agency, by year

Initiative	Year	$m
Department of Justice – *continued*		
Establish Emergency Management Exercise Group to organise and coordinate regular counter-terrorism and emergency management exercises	2006–07	1.80
Subtotal		***69.17***
Department of Premier and Cabinet		
Creation of a dedicated State Crisis Centre with secure communications	2002–03	4.00
Recurrent funding for Security and Emergencies Unit within DPC ($500 000 per annum)	2002–03	3.00
Enhanced security at Parliament House and Government House	2003–04	3.60
Further security enhancements at Parliament House	2004–05	0.25
Additional State Crisis Centre operational funding	2005–06	1.60
Public information campaigns to improve the Victorian community's awareness of counter-terrorism and transport security arrangements	2006–07	2.50
State Crisis Centre additional staff	2006–07	2.90
Establishment of a Global Terrorism Research Centre at Monash University	2006–07	1.20
Extra funding for the Centre for Dialogue, La Trobe University	2006–07	0.27
Research into the most effective counter-terrorism technology and equipment—National Research and Development Fund	2006–07	0.40
Subtotal		***19.72***
Department of Primary Industries		
Department business resilience	2004–05	1.20
State Chemical Laboratory capacity	2004–05	2.05
Establishment of a National Biosecurity Centre	2005–06	5.77
Regional officers to enhance plant biosecurity	2005–06	8.40
Energy sector counter-terrorism risk audits	2006–07	0.40
Subtotal		***17.82***
Department of Sustainability and Environment		
Upgrade VicMap datasets	2003–04	11.50
Geospatial Emergency Information Network feasibility study	2003–04	0.25
Subtotal		***11.75***
Department of Transport		
Public transport security, including maintenance of security cameras	2006–07	21.00
Installation of a public radio re-broadcasting system in the City Loop	2006–07	1.00
Motorised rail trolleys for the City Loop	2006–07	0.49
Subtotal		***22.49***

Figure A1 – *continued*

Funding allocated for counter-terrorism related initiatives, by agency, by year

Initiative	Year	$m
Victoria Police		
Establish Counter-Terrorism Coordination Unit	2002–03	12.00
Surveillance and communications to increase intelligence and risk analysis capacity	2002–03	3.80
Enhancement of Special Operations Group capability to manage bomb threat, hostage and kidnap scenarios	2002–03	5.00
Protective clothing and equipment for response to chemical biological and radiological incidents	2002–03	1.20
Upgrade forensic equipment	2002–03	1.00
Increase IT capacity to ensure Vic Pol operations cannot be interrupted through a targeted terrorist attack	2002–03	6.40
Intelligence and investigation capabilities	2004–05	13.51
Enhanced water police capability for port security	2005–06	16.00
Extra counter-terrorism staff and resources for Security Intelligence Group	2006–07	3.50
Ballistic-rated vehicle for Special Operations Group	2006–07	0.40
Mobile Closed Circuit Television Van	2006–07	0.25
Port security	2008–09	19.00
Subtotal		***82.06***
Total		**255.00**

Source: Selected agencies and Department of Treasury and Finance, *Budget Paper No. 3* 2002-03 to 2008–09.

Appendix B.

CIP framework roles and responsibilities of lead departments

Figure B1
CIP framework roles and responsibilities of lead departments, April 2007

Roles and responsibilities	DHS	DIIRD	DOJ	DPI	DSE	DOT
Participate in and support the national CIP arrangements through relevant IAAGs	✓	✓	✓	✓	✓	✓
Chair relevant sector SCN	✓	✓	✓	✓	✓	✓
Disseminate non-time critical information to owners/operators	✓	✓	✓	✓	✓	✓
Provide strategic advice to government and coordination across the relevant sector to achieve sufficient capacity and preparedness to respond to emergencies, as well as support national CIP arrangements		✓		✓		✓
Risk management advice to owners/operators of declared essential services in managing compliance with the obligations under the TCP Act						✓
Risk management advice to owners/operators of CIP (non-declared) in the application of this CIP framework						✓
Incident and emergency management coordination for the portfolio in support of whole-of-government matters, including business continuity planning						✓
Provide leadership for protection of critical infrastructure in the sector					✓	
Act as the control agency during incidents and emergencies					✓	
Ensure sector compliance with policy and regulatory requirements, particularly in the area of emergency management and protection of critical infrastructure					✓	
Work with Emergency Service Operators (ESOs) to ensure they have protective arrangements in place to protect associated key facilities			✓			
Work with ESOs to develop relevant capabilities for CIP and ensure continuity of service			✓			
Provide emergency management and business continuity advice across the sector as required			✓			
Participate in various other sector SCNs	✓					
Provide guidelines to operators of CI facilities on security arrangements relative to standards and guidelines	✓					
Provide assistance and advice in the development and maintenance of business continuity and contingency planning for CI facilities	✓					
Establish and maintain design guidelines for the development of CI facilities with specific requirements for security and safety	✓					
Provide advice and support to operators of CI facilities including essential engineering infrastructure such as emergency electricity and water supply to ensure continued health care service delivery	✓					
Develop tools for assessing contamination risk for water supplies from chemicals	✓					
Coordinate all department emergency response and recovery arrangements	✓					
Liaise with state and national agencies, including Victoria Police on security and emergency management matters	✓					

Figure B1 – *continued*

CIP framework roles and responsibilities of lead departments, April 2007

Roles and responsibilities	DHS	DIIRD	DOJ	DPI	DSE	DOT
Liaise with DPC on state security issues and notify operators of critical infrastructure on threat information and relevant actions required	✓					
Contribute to adequate management of security risks and emergencies for relevant sectors		✓		✓		✓
Participate, in line with the development of emergency response plans under the state emergency framework, in a coordinated whole of government approach to the development and revision of strategies to protect Victoria's primary industry infrastructure from the impact of pests, diseases and chemical residues, whether naturally occurring or through human intervention				✓		
Carry out appropriate investigations and response activities from farm to processing for pest, disease and chemical residue incidents or incursions to Victoria's primary industries				✓		
Cooperate and liaise with other agencies to ensure consistency while implementing as far as practicable, preventative and emergency response activities, control and relief and recovery				✓		
Ensure a consistent media response and communicate information and decisions to other agencies and individuals as required, quickly and clearly				✓		
Test its whole of government management plans regularly, with a view to refining and improving those plans as required				✓		
Participate in regular testing of national whole of government management plans for emergency pest and disease containment responses				✓		
Interest in water threat assessment in relation to the surety and quality of water	✓					
Responsible for food safety	✓					

Source: Victorian Framework for Critical Infrastructure Protection from Terrorism, April 2007.

Legend

✓	Yes
DHS	Department of Human Services
DIIRD	Department of Innovation, Industry and Regional Development
DOJ	Department of Justice
DPI	Department of Primary Industries
DSE	Department of Sustainability and Environment
DOT	Department of Transport

Appendix C.

Response from Acting Secretary, Department of Premier and Cabinet

SPECIFIC COMMENTS RELATING TO THE VAGO PREPAREDNESS AUDIT REPORT OF CRITICAL INFRASTRUCTURE

We note that the main focus of the Report is on the governance arrangements established to assist operators of essential services and owners/operators of critical infrastructure to respond to terrorism incidents. The public sector's preparedness to respond and recover was not in scope of the Report.

The Report acknowledges that Victoria was an early mover to develop means to protect essential services and critical infrastructure following the 2001 terrorist attacks.

DPC acknowledges that all innovations require review and further development once they have been in place for a period and will use the VAGO report to assist with this process.

DPC also notes that the provisions in part 6 of the Terrorism (Community Protection) Act 2003 relating to mandatory risk management activities for declared essential services are unique in Australia. They provide an additional set of requirements beyond the agreed voluntary national guidelines.

We note that the most significant critical infrastructure sectors in Victoria are energy, transport and water. We note further that VAGO has found the arrangements are working effectively in relation to these sectors.

However, DPC would like to raise the following comments in the context of the Report. These comments are in addition to the detailed comments previously provided in response to the iterations of the audit report:

- *Victoria's arrangements for the security of essential services have evolved through successive governments and a number of reviews commencing in 1999. These reviews defined essential services and assessed the sectors that required the highest level of protection. The report does not appear to acknowledge these seminal reviews and their influence in establishing policy, strategy and the form of the legislation.*

- *The assessment of risk, threat and vulnerability are important factors that enable decisions and practice to protect the community and services that are essential for the normal functioning of the community. Government declares essential services under Part 6, of the Terrorism (Community Protection) Act 2003, to ensure owners and operators manage their risk. Government's role is to assist. If Government takes a more prescriptive role, the private sector could transfer risk to Government which would not be a good policy outcome. This is a significant issue because the purpose of the arrangements is to manage risk for Government and the community. The services that have been declared (water, transport, and energy) are the sectors that Australia's intelligence agencies have consistently assessed as the highest risk.*
- *The main driver for the legislation was to enable Government to require public utilities that had previously been under Government control, to undertake risk management planning to counter a terrorist attack.*
- *Essential services were defined in 2002 Review of Security of Supply of Essential Services as "services which, if disrupted would substantially disrupt normal life for a significant sector of the community". Services determined as meeting this definition were water, gas, electricity, telecommunications, financial services, transport, fuel, emergency information, Melbourne Airport and Cabinet and Parliament services. Where Government has direct control of a service provider, and there is low likelihood of service disruption due to such elements as alternate delivery routes or a diffuse service delivery network, there is no need to declare a service as an essential service. Therefore, not all infrastructure sectors need to declare essential services*
- *Many organisations operate nationally which means the arrangements in States and Territories should be the same or similar and link seamlessly to national arrangements. This has affected the structure and content of Victoria's Framework. The Commonwealth, through a COAG decision in 2004, assumed responsibility for protecting the industries it regulates, including banking and finance, communications and aviation. Victoria supports national efforts in these industries rather than duplicate them.*

Points of clarification

As identified to VAGO, Part 6, of the Terrorism (Community Protection) Act 2003, mandates specific requirements for those critical infrastructure elements that, due to their criticality, are declared essential services. All essential services are critical infrastructure, but not all critical infrastructure is an essential service. Under Part 6, 'declared essential services' are specific services that a responsible Minister considers requires protection from terrorism through the implementation of mandatory risk management planning. Part 6 defines the services that can be declared, including transport, power and water services. The decision to declare an essential service includes consideration of the risk, vulnerability, threat and consequences of disruption. In making a declaration the Minister is required to specify which service, or which specific part of a service, is being declared. In this way, the relevant Minister has not declared all transport services only those that, if disrupted, would result in substantial disruption for a significant sector of the community. This variability particularly applies to transport where some aspects such as the train network has few alternatives, but the tram and bus system can be reconfigured to minimise disruption.

The following table outlines how declared essential services, critical infrastructure sectors and services have been protected.

PROTECTION OF CRITICAL INFRASTRUCTURE AND ESSENTIAL SERVICES			
C. I. SECTOR	***SERVICE***	***OWNERSHIP / CONTROL***	***COMMENT***
Includes essential services declared under Terrorism (Community Protection) Act 2003			
Transport *Included in 2002 Security of Supply Review*	*Trains, trams, buses,* *Roads and bridges*	*Private sector* *Principally State*	*Trains declared essential service. Trams and buses have alternatives. Participate in national IAAG. SCN active.* *Critical bridge declared essential service*
Water *Included in 1999 and 2002 Security of Supply Reviews*	*Water supply, storage and sewerage*	*State corporations*	*Declared essential services. Participate in national IAAG. SCN active.*
Energy *Included in 1999 and 2002 Security of Supply Reviews*	*Electricity generation, transmission and distribution*	*Private Sector*	*Declared essential services. Participate in national IAAG. SCN active.*

C. I. SECTOR	SERVICE	OWNERSHIP / CONTROL	COMMENT
Subject to Commonwealth legislation and control – COAG decision 2004			
Communications Included in 2002 Security of Supply Review	Telephone, internet, radio and television broadcast	Private Sector	Government regulated industries, Commonwealth legislation likely to leave no scope for state legislation, attempting to activate SCN to coordinate locally
Banking and Finance Included in 2002 Security of Supply Review	Banking, stock exchange, lending institutions	Private Sector	Government regulated industries, Commonwealth legislation likely to leave no scope for state legislation, attempting to activate SCN to coordinate locally
SCN's developing			
Health	Hospitals and supporting services	State and Private Sector	Commonwealth and State regulated. Have utilised all hazards emergency risk plans. SCN launched.
Food Supply	Production, processing, distribution and sale	Private Sector	Dept of Primary Industries participates on national IAAG. Considering activating SCN
Protection undertaken via reporting to the Minister for Police & Emergency Services via the Victoria Emergency Management Council			
Emergency Services Included in 1999 and 2002 Security of Supply Reviews	Police, fire, ambulance, state emergency services, and support services	State	Utilising all hazards emergency risk plans and report business continuity to Minister for Police and Emergency Services through the Victoria Emergency Management Council
Not infrastructure, included for consistency with national arrangement			
Mass Gatherings	Festivals, sporting events, shopping centres and places of entertainment	State, Community and Private Sector	State regulation. Police and private security providers have well developed security and emergency plans for all major public events. Legislation for specific events also applies. Victoria Police has an international reputation for effective major event security.

VAGO advocates a role that DPC should perform in the arrangements that is different to that which DPC believes it should undertake. Part 6 of the Terrorism (Community Protection) Act 2003 is administered by the Premier. The Premier (and DPC) are therefore responsible for ensuring that the provisions operate as intended and for updating and amending the legislation if required. In this role, DPC has reviewed Part 6 in a broader review of the operation of the Act.

Part 6 provides that the Premier designate responsible ministers who are then responsible for a variety of activities. The Premier has written to Ministers to advise them of their responsibilities as 'relevant Ministers' under the Act. The Ministers have accepted their roles and responded to the Premier that they will monitor and ensure compliance with Part 6 requirements. This ensures Ministers, and agencies with relevant executive authority and subject matter expertise, consider the implementation of the Act. As supported by international best practice, this is preferable to implementation of a "one size fits all" approach.

Interpretation of legislation

When referring to Part 6 provisions the report ascribes a definition to essential services and the purpose of the provisions that differs from the wording of the Act. A description of what is mandated under the Act is also different to the wording of the Act. Similarly, a description that a Minister can 'delegate his or responsibilities (under Part 6) to public servants is incomplete and does not recognise that the Part specifically notes that some of the powers cannot be delegated, including the critical power to recommend to the Governor in Council that an essential service be declared. The omitted clauses could lead a reader to gain an incorrect or incomplete understanding of the Part.

In its recommendation seeking declaration of further essential services, VAGO has not discussed the interaction between Commonwealth and State legislative power. The Commonwealth regulates financial institutions under the Banking Act 1959 (Cwth) and its regulations have covered the field (including through the issue of prudential standards and guidelines covering Risk Assessment and Business Continuity Management). Similarly the audit does not recognise that the Telecommunications Act 1997 (Cwth) places obligations on carriers and carriage service providers during crises. There does not appear to be scope for the State to regulate in this area, nor would it be useful to replicate arrangements already operating effectively. The Council of Australian Governments agreed in 2004 that the Commonwealth would assume responsibility for planning and monitoring protection of critical infrastructure in sectors it regulates.

Security policy across Australia is subject to constant and continuing review.

RESPONSE TO AUDIT RECOMMENDATIONS

The Department of Premier and Cabinet offers the following responses to the recommendations of the audit report:

The Department of Premier and Cabinet should:

1. ***establish clear oversight and coordination of the arrangements for both Part 6 of the Terrorism (Community Protection) Act 2003 (the Act) and the CIP Framework by an appropriate body, such as the Government Security and Continuity Network Coordination Group with expanded responsibilities (Recommendation 4.1).***

   DPC will consider the intent of the recommendation in its current review noting however, that it would be against best practice for DPC to undertake an operational role in the management of these activities.

2. ***lead the development of a performance management framework for measuring, monitoring and reporting on the implementation of Part 6 of the Act and the CIP Framework. The framework should include key indicators, targets and reporting arrangements for assessing the extent to which departments, agencies and industry have fulfilled their obligations, as well as measures for monitoring achievement of joint objectives (Recommendation 4.2).***

   Victoria has developed devolved arrangements that make owners and operators and relevant Ministers and departments responsible for monitoring the compliance with the Act and framework in accordance with best practice. DPC will however consider the intent of the recommendation in its current review.

3. ***clarify the roles and responsibilities of departments and agencies under Part 6 of the Act and CIP Framework to reduce confusion and gaps (Recommendation 4.3).***

   The roles and responsibilities of relevant parties to the arrangements will be revisited in the review of the CIP arrangements (including Part 6) that is currently being undertaken by DPC. In addition, Victoria has proposed to the Commonwealth that a review of the national arrangements be undertaken to clarify roles, responsibilities and definitions.

4. ***provide definitive guidance on identifying essential services for declaration to better inform relevant departments in discharging their responsibilities under Part 6 of the Act (Recommendation 4.4).***

The 2002 Review of the Security of Supply of Essential Services defined essential services. This definition has been agreed by Government and underpins the arrangements in place in Victoria. The finding of the audit that the three most critical sectors have been effectively declared and managed demonstrates that the declaration process is working effectively. DPC will cover the recommendation and its intent in its current review.

5. ***identify risks arising from the joined-up nature of the approach to protecting essential services and critical infrastructure and to assist departments and agencies to develop associated risk management arrangements at the whole of government level (Recommendation 4.5).***

   A coordinated, whole of government approach is generally regarded as best practice for ensuring consistent policy and arrangements across a range of participating agencies. We also note that the recent Commonwealth review, released as part of the National security Statement, included that the Commonwealth is moving to a more joined –up approach to domestic security which is consistent with the Victorian approach. DPC will cover the recommendation and its intent in its current review.

6. ***clarify the requirements in relation to establishing Security and Continuity Networks in designated sectors, so that there is a shared understanding of those requirements (Recommendation 4.6).***

   DPC accepts the recommendation and will cover the appropriate mechanisms in its review.

7. ***Representatives of lead departments should obtain necessary security clearances so appropriate officers can access information relevant to their sectors (Recommendation 4.7).***

   DPC strongly supports this recommendation. At the end of 2007 DPC promulgated policies to achieve this end.

8. ***The Department of Premier and Cabinet, in consultation with Victoria Police, should develop clear guidance to distinguish between declared essential services and critical infrastructure to assist departments, Victoria Police and industry in implementing Part 6 of the Act and the CIP Framework more effectively (Recommendation 5.1).***

   Please see response to recommendation 4 above.

9. ***The Department of Premier and Cabinet should provide clear guidance on terms such as 'audit', 'auditor' and 'adequacy of the exercise' to assist departments, Victoria Police and industry to implement requirements more reliably (Recommendation 5.2).***

   The best method to ensure guidance on the issue of terminology and definitions will be covered in the review of the CIP arrangements (including Part 6) that is currently being undertaken by DPC.

10. ***The Department of Premier and Cabinet and Victoria Police, in consultation with departments, should standardise reporting on training exercises conducted under Part 6 of the Act and the CIP Framework to promote greater consistency and to enable better identification of lessons learned and continuous improvement (Recommendation 5.3).***

    The Victorian Government in October 2006 announced the creation and funding of a centralised exercise management group within the Office of the Emergency Services Commissioner, to co-ordinate counter-terrorism and emergency management exercises. This role includes maintaining a record of the outcomes of exercises to aid continual improvement. DPC will cover this recommendation in the review currently being undertaken.

11. ***Reports on the training exercises should be retained in an appropriately secured central repository so that consolidated reports of the exercises can be drawn together effectively (Recommendation 5.4).***

    See response to previous recommendation. DPC has promulgated guidance on standards for securing security classified information.

Appendix D. Glossary

Critical infrastructure

Under the *Victorian Framework for Critical Infrastructure Protection from Terrorism*, critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of Victoria and its community.

Essential services

Under Part 6 of the *Terrorism Community Protection Act 2003* (the Act), essential services are transport, fuel (including gas), light, power, water, sewerage and a service declared to be an essential service by the Governor-in-Council under the Act.

Government Security and Continuity Network Coordination Group

The Government Security and Continuity Network Coordination Group is comprised of the Chairs of all Security and Continuity Networks, a representative from Victoria Police's Critical Infrastructure Protection Unit and a representative from the Department of Premier and Cabinet's Security and Emergencies Unit. Its role includes oversight of the Security and Continuity Networks, producing guidance on critical infrastructure protection developments in each sector, and reporting to the Central Government Response Committee on the operation of the networks.

Infrastructure Assurance Advisory Groups

Infrastructure Assurance Advisory Groups are trusted information sharing networks created under the *Critical Infrastructure Protection National Strategy* for the national critical infrastructure sectors. The Infrastructure Assurance Advisory Groups are overseen by the Critical Infrastructure Advisory Council.

Lead department

Under the *Victorian Framework for Critical Infrastructure Protection from Terrorism*, 'lead' departments have key roles and responsibilities that support the protection of critical infrastructure. The *Victorian Framework for Critical Infrastructure Protection from Terrorism* document published in April 2007 sets out specific roles and responsibilities of lead departments.

National critical infrastructure sectors

The nine national critical infrastructure sectors are banking and finance, communications, emergency services, energy, food chain, health, icons and public gatherings, transport, and water services.

Relevant department

A relevant minister may delegate his or her responsibilities under Part 6 of the *Terrorism Community Protection Act 2003* to public servants. The department that carries the delegation from the relevant minister is referred to as the 'relevant department'.

Relevant minister

Under Part 6 of the *Terrorism Community Protection Act 2003*, the Premier may designate a 'relevant minister' for an essential service. The Act mandates particular activities to the relevant minister in relation to the essential service, including recommending declaration of essential services, advising operators that their essential services have been 'declared', setting timeframes for preparation of risk management plans by operators, determining intervals for operators to prepare and participate in training exercises, and consulting on the form and content of reports on training exercises.

Security and Continuity Network

The *Victorian Framework for Critical Infrastructure Protection from Terrorism* provides for the establishment of a Security and Continuity Network (SCN) for each of the nine critical infrastructure sectors, to bring together state and local government representatives and owners/operators of critical infrastructure to consider relevant security, emergency management and business continuity policies and practices. Each SCN is chaired and administered by the designated lead department.

Victorian critical infrastructure sectors

The nine Victorian critical infrastructure sectors are: banking and finance, communications, energy, food supply, health, places of mass gathering, police and emergency services, transport and water.

Auditor-General's reports

Reports tabled during 2008–09

Report title	Date tabled
Managing Complaints Against Ticket Inspectors (2008–09:1)	July 2008
Records Management Checklist: A Tool to Improve Records Management (2008–09:2)	July 2008
Investing Smarter in Public Sector ICT: Turning Principles into Practice (2008–09:3)	July 2008
Private Practice Arrangements in Health Services (2008–09:4)	October 2008
Working with Children Check (2008–09:5)	October 2008
CASES21 (2008–09:6)	October 2008
School Buildings: Planning, Maintenance and Renewal (2008–09:7)	November 2008
Managing Acute Patient Flows (2008–09:8)	November 2008
Biosecurity Incidents: Planning and Risk Management for Livestock Diseases (2008–09:9)	November 2008
Enforcement of Planning Permits (2008-09:10)	November 2008
Auditor-General's Report on the Annual Financial Report of the State of Victoria, 2007–08 (2008–09:11)	November 2008
Local Government: Results of the 2007–08 Audits (2008–09:12)	November 2008
Management of the Multi-Purpose Taxi Program (2008–09:13)	December 2008
Results of Audits for Entities with 30 June 2008 Balance Dates (2008–09:14)	December 2008

VAGO's website at <www.audit.vic.gov.au> contains a more comprehensive list of all reports. The full text of the reports issued is available at the website. The website also features 'search this site' and 'index of issues contained in reports and publications' facilities that enable users to quickly identify issues of interest which have been commented on by the Auditor-General.

VAGO

Victorian Auditor-General's Office

Auditing in the Public Interest

Availability of reports

Copies of all reports issued by the Victorian Auditor-General's Office are available from:

- Information Victoria Bookshop
  505 Little Collins Street
  Melbourne Vic. 3000
  AUSTRALIA

  Phone: 1300 366 356 (local call cost)
  Fax: +61 3 9603 9920
  Email: <bookshop@diird.vic.gov.au>

- Victorian Auditor-General's website: www.audit.vic.gov.au.