PUBLIC ACCOUNTS AND ESTIMATES COMMITTEE

105TH REPORT TO THE PARLIAMENT

Review of the Auditor-General's Report on Preparedness to Respond to Terrorism Incidents: Essential Services and Critical Infrastructure

December 2011

Ordered to be
printed

By Authority
Government Printer for the State of Victoria

No. 67
Session 2010-11

PUBLIC ACCOUNTS AND ESTIMATES COMMITTEE

Address:	Parliament of Victoria Spring Street East Melbourne Victoria 3002
Telephone:	+61 3 8682 2867
Facsimile:	+61 3 8682 2898
Email:	paec@parliament.vic.gov.au
Web:	www.parliament.vic.gov.au/paec

Parliament of Victoria
Public Accounts and Estimates Committee

Review of the Auditor-General's Report on Preparedness to Respond to Terrorism Incidents: Essential Services and Critical Infrastructure

ISBN 978 0 9871550 1 6

CONTENTS

PUBLIC ACCOUNTS AND ESTIMATES COMMITTEE MEMBERSHIP — 57TH PARLIAMENT

Philip R. Davis MP (Chairman)

Martin Pakula MLC (Deputy Chair)

Neil Angus MP

Jill Hennessy MP

David Morris MP

David O'Brien MLC

Robin Scott MP

For this inquiry, the Committee was supported by a secretariat comprising:

Executive Officer:	Valerie Cheong
Senior Research Officer:	Leah Brohm
Business Support Officer:	Melanie Hondros
Desktop Publisher:	Justin Ong

DUTIES OF THE COMMITTEE

The Public Accounts and Estimates Committee is a joint parliamentary committee constituted under the *Parliamentary Committees Act 2003*.

The Committee comprises seven members of Parliament drawn from both Houses of Parliament.

The Committee carries out investigations and reports to Parliament on matters associated with the financial management of the State. Its functions under the Act are to inquire into, consider and report to the Parliament on:

- any proposal, matter or thing concerned with public administration or public sector finances;
- the annual estimates or receipts and payments and other budget papers and any supplementary estimates of receipts or payments presented to the Assembly and the Council; and
- any proposal, matter or thing that is relevant to its functions and has been referred to the Committee by resolution of the Council or the Assembly or by order of the Governor in Council published in the Government Gazette.

The Committee also has a number of statutory responsibilities in relation to the Office of the Auditor-General. The Committee is required to:

- recommend the appointment of the Auditor-General and the independent performance and financial auditors to review the Victorian Auditor-General's Office;
- consider the budget estimates for the Victorian Auditor-General's Office;
- review the Auditor-General's draft annual plan and, if necessary, provide comments on the plan to the Auditor-General prior to its finalisation and tabling in Parliament;
- have a consultative role in determining the objectives and scope of performance audits by the Auditor-General and identifying any other particular issues that need to be addressed;
- have a consultative role in determining performance audit priorities; and
- exempt, if ever deemed necessary, the Auditor-General from legislative requirements applicable to government agencies on staff employment conditions and financial reporting practices.

ACRONYMS AND ABBREVIATIONS

AS/NZS	Australian/New Zealand Standard
ASIO	Australian Security Intelligence Organisation
The Act	The Terrorism (Community Protection) Act 2003
CGEIG	Central Gippsland Essential Industries Group
CGRC	Central Government Response Committee
CIP	Critical Infrastructure Protection
CIP policy Framework	Victorian Framework for Critical Infrastructure Protection from Terrorism
CIPMA	Critical Infrastructure Protection Modelling and Analysis
CIPU	Critical Infrastructure Protection Unit
COAG	Council of Australian Governments
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DBI	Department of Business and Innovation
DIIRD	Department of Innovation, Industry and Regional Development
DOH	Department of Health
DOJ	Department of Justice
DOT	Department of Transport
DPC	Department of Premier and Cabinet
DPC Review Report	Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure
DPI	Department of Primary Industries
DSE	Department of Sustainability and Environment
DTF	Department of Treasury and Finance
EMA	Emergency Management Australia
EMTESC	Emergency Management Training and Exercising Strategy Committee
ENA	Energy Networks Association
ESTA	Emergency Services Telecommunications Authority

ESV	Energy Safe Victoria
FSA	Formal Safety Assessment
ICT	Information and Communication Technology
ISO	International Standards Organisation
Minister for Finance Report	Response by the Minister for Finance to the Auditor-General's Reports 2008-09
NCTC	National Counter-Terrorism Committee
NCTP	National Counter-Terrorism Plan
OESC	Office of the Emergency Services Commissioner
OHS	Occupational Health and Safety
PAEC	Public Accounts and Estimates Committee
SCADA	Supervisory Control and Data Acquisition
SCN	Security and Continuity Network
SCN-CG	Security and Continuity Network-Coordination Group
SECC	Security and Emergencies Committee of Cabinet
SHERP	State Health Emergency Response Plan
SMS	Safety Management System
TISN	Trusted Information Sharing Network
VMIA	Victorian Managed Insurance Authority

CHAIRMAN'S FOREWARD

Under its functions and powers set out in sections 14 and 33 of the *Parliamentary Committees Act 2003*, the Public Accounts and Estimates Committee follows-up the status of findings and recommendations made in a selection of priority audit reports tabled in the Parliament by the Victorian Auditor-General.

In January 2009, the Auditor-General tabled a report entitled *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*. This report was selected by the Committee for Inquiry due to the significance of the area in terms of public interest and significance to the State's security and economy.

Critical infrastructure is a term used to describe assets and services which are essential to the functioning of a society and an economy and extend across many industry sectors such as energy, water, communications, transport, emergency services, banking and finance and public health. A significant proportion of Victoria's critical infrastructure and essential services are owned and or operated by private sector organisations. As such, former Victorian Governments have sought to influence the protection of these assets and services through legislation and policy.

In Victoria, Part 6 of the *Terrorism (Community Protection) Act 2003* contains statutory requirements on the part of operators of declared essential services to prepare and test risk management plans which specifically address the risk of a terrorist incident. Part 6 is administered by the Premier through the Department of Premier and Cabinet.

In April 2007, the Department of Premier and Cabinet issued the *Victorian Framework for Critical Infrastructure Protection from Terrorism* (CIP policy Framework) which establishes guiding principles and coordination arrangements for government and industry to develop joint strategies to protect the State's critical infrastructure.

The Committee's Inquiry is historical in nature and has focussed on actions taken since the tabling of the Auditor-General's report to address the issues and recommendations made. In forming its conclusions and recommendations, the Committee has used evidence provided by the Department of Premier and Cabinet and the Department of Justice, including Victoria Police and the Office of the Emergency services Commissioner. Additional comments were also sought from the Auditor-General. Consideration was also given to COAG agreed national strategies and policies.

The Committee was disappointed with the position taken by the Department of Premier and Cabinet in regard to its critical infrastructure protection oversight and governance responsibilities. The Committee is of the view that the Department continues to dispute its obligations and responsibilities in coordinating the effective oversight of the application of Part 6 of the Act and the CIP policy Framework by relevant departments. Further, the Committee considers that, as a consequence of this ongoing lack of acceptance of its responsibilities as alerted to by the Auditor-General and now, the Committee, the Department has not adequately supported the Premier, as head of Government and, "Minister" ultimately responsible and accountable to Parliament and the Community for critical infrastructure protection arrangements across the whole-of-government. The implications of this deficiency have not yet been tested due to the absence of a relevant incident to date. The report discusses this issue comprehensively.

The Committee's conclusions on the adequacy of the Department of Premier and Cabinet's oversight arrangements affirm the findings and concerns expressed by the Auditor-General in his report of January 2009. This is a continuing concern to reviewers of the Victorian CIP framework. The Committee was surprised that it remains an outstanding issue given the Auditor-General's earlier observations. The Committee further noted that the Auditor-General confirmed his concerns in evidence at the Committee's Public Hearings on this Inquiry.

The challenge in critical infrastructure protection management for government in the future is to address the issues identified and lessons learned from the last few years' operation of Part 6 of the *Terrorism (Community Protection) Act 2003* and the CIP policy Framework. In addition, developments in national policy and changes in the risk environment have highlighted new issues which must be taken into consideration in order that requirements remain meaningful and relevant.

The Committee is of the view that to improve public sector administration of critical infrastructure protection arrangements there is a need for:

- the provision of clear and strong central policy leadership and coordination even within a "devolved" system of responsibility;
- clearly and commonly understood, terminology and definitions, and roles and responsibilities of all stakeholders;
- a formalised process for the identification and classification of critical infrastructure (including essential services);
- standardised application of CIP requirements across categories of "criticality";
- the consideration of all risks, and in particular other "high/catastrophic impact", "low probability" risks;
- a formal and standardised system of certification and reporting; and
- incorporation of the COAG agreements on a uniform approach to disaster management resilience and critical infrastructure protection.

The opportunity to address these issues presents now in the redrafting of the *Victorian Framework for Critical Infrastructure Protection from Terrorism* policy document and also in the forthcoming review of the *Terrorism (Community Protection) Act 2003*, due for completion in June 2013.

It is hoped that the recommendations put forward by the Committee in this follow-up inquiry to the Auditor-General's report will assist in improving the management of critical infrastructure protection arrangements across the Victorian public sector in the future.

The Committee has been assisted in its inquiry by evidentiary support from the Department of Premier and Cabinet, Department of Justice, Victoria Police, the Office of the Emergency Services Commissioner and the Victorian Auditor-General's Office and I thank them for their advice and assistance.

This report would not have been possible without the commitment and dedication of the Secretariat staff, who again have ensured an exceptionally professional standard of research.

Philip R. Davis

Philip R. Davis MP
Chairman

FINDINGS AND RECOMMENDATIONS OF THE COMMITTEE

CHAPTER 1 – BACKGROUND TO THE INQUIRY

Section 1.6.1 – Funding for counter-terrorism initiatives

The Auditor-General reported that between October 2002 and June 2009, around $255 million had been allocated to counter-terrorist arrangements and activities in Victoria.

. . . . .page 4

Since 2008, funding for counter-terrorism arrangements have been absorbed into the general budget of the State government rather than appearing as a separate line item.

. . . . .page 4

The Department of Justice advised that between June 2009 and June 2012, general emergency services funding totalling $474.8 million has been allocated for initiatives in the Department's emergency services area which, whilst not specifically assigned to counter-terrorism preparedness, provide assets and services which would be called upon in response to a terrorist incident.

. . . . .page 4

The Committee notes the current difficulty in isolating the amount of funding provided specifically for counter-terrorist activities and preparedness in the State, but looks forward to the possibility of these funds being separately identified to allow for greater transparency and assist in assessing the effectiveness of such funding.

. . . . .page 4

Recommendation 1:

The Committee recommends that, to enhance transparency, the Department of Treasury and Finance consider issuing Financial Reporting Directions requiring all departments and agencies to identify and report within their Annual Reports funding allocated for counter-terrorism initiatives and activities, such as preparedness training, risk management and support to industry and other relevant stakeholders.

. . . . .page 5

CHAPTER 4 - GOVERNANCE AND ACCOUNTABILITY

Section 4.4.1 – Oversight and coordination of critical infrastructure protection arrangements

The role of the Department of Premier and Cabinet and the level of appropriate oversight by the Department of the critical infrastructure protection arrangements in the State were the main points of contention between the Auditor-General and the Department during the audit review.

. . . . page 39

The Department of Premier and Cabinet view their role in managing the protection of critical infrastructure as strictly one of strategic leadership on policy and legislative advice. Responsibility and accountability for the effectiveness of the arrangements is devolved to relevant Ministers and their departments. The Department's involvement in monitoring and oversight is based largely in its chairing of the Security and Continuity Network-Coordination Group and the Central Government Response Committee.

. . . . page 39

The Auditor-General has concerns about "oversight deficit" by agencies responsible for policy development but not directly involved with the implementation of policy. And, in the case of critical infrastructure protection arrangements, the Auditor-General continues to express concerns about executive responsibility and leadership on the part of the Department of Premier and Cabinet.

. . . . pages 40, 42

Critical infrastructure protection (CIP) governance and accountability arrangements, as have been operating, are seriously lacking in terms of the adequacy of central monitoring and oversight of the application of Part 6 of the *Terrorism (Community Protection) Act 2003* and the CIP policy Framework across public sector agencies.

. . . . page 47

The Department of Premier and Cabinet has not accepted and continues to dispute their obligations and responsibilities in co-ordinating the effective application and implementation of Part 6 of the *Terrorism (Community Protection) Act 2003* and the requirements and principles outlined in the *Victorian Framework for Critical Infrastructure Protection from Terrorism* (the CIP policy Framework).

. . . . page 47

There remains a persistent reluctance on the part of the Department of Premier and Cabinet in accepting ultimate accountability for critical infrastructure protection arrangements in the State in line with its role as the agency primarily responsible for the administration of Part 6 of the Act and the agency responsible for the development of critical infrastructure policy in the State.

. . . . page 48

Responsibility for the effective application of critical infrastructure protection legislation and policy cannot be completely devolved to either Victoria Police or to individual departments. The Department of Premier and Cabinet must be accountable and must desist from continuing to avoid its obligations and responsibilities in this area by taking much stronger action to monitor performance, provide guidance and encourage compliance across Victorian public sector agencies and amongst industry stakeholders.

. . . . .page 48

Recommendation 2:

The Committee recommends that, as a matter of good governance and due and proper accountability and assurance, the Department of Premier and Cabinet take a greater lead in providing guidance and monitoring compliance as part of their strategic responsibilities for the oversight of critical infrastructure protection arrangements in Victoria. Such strategic oversight and monitoring should include:

(a) An appropriate system of internal accountability between itself and departments/agencies implementing the *Victorian Framework for Critical Infrastructure Protection from Terrorism* policy and the provisions of Part 6 of the *Terrorism (Community Protection) Act 2003*;

(b) The identification of the key critical infrastructure protection policy outcomes and performance measures against which the effectiveness of departments' and agencies' critical infrastructure protection arrangements can be assessed; and

(c) A comprehensive reporting system to enable monitoring of outcomes and the status of implementation across departments/ agencies to identify factors impacting upon the desired outcomes and areas for improvement.

. . . . .page 49

Recommendation 3:

The Committee recommends that the critical infrastructure protection management structure as depicted in the Department of Premier and Cabinet's policy documentation be revised. Such revision should clearly show the Department of Premier and Cabinet as the agency ultimately responsible for overseeing management arrangements across the whole-of-government for the protection of both critical infrastructure and declared essential services and their responsibility to the Premier as the "Minister" accountable to the Parliament for these arrangements.

. . . . .page 49

Section 4.4.2 – Development of a performance management framework

The Department of Premier and Cabinet has not taken action to address the Auditor-General's recommendation for the development of a performance management framework for monitoring and reporting on Part 6 of the Act and the CIP policy Framework. The Department of Premier and Cabinet maintains that performance monitoring is an "operational responsibility" not a "strategic" one and therefore is devolved to the relevant Ministers and their departments.

. . . . page 50

The Department of Premier and Cabinet has not developed any specific performance indicators, targets, key measures or formalised reports to assess its performance in the area of critical infrastructure protection. The Department considers that the devolved nature of critical infrastructure protection arrangements makes it difficult to quantify or measure its own performance.

. . . . page 52

There is very little evidence that any serious consideration has been afforded the Auditor-General's recommendation relating to the development of a performance management framework to assess the implementation and effective operation of the CIP policy Framework.

. . . . page 54

There is some formal documentation and recording in place by Victoria Police and in those departments overseeing the better established industry sectors such as water, energy and transport in relation to their statutory obligations under Part 6 of the Act.

. . . . page 54

The Committee was unable to assess the extent or quality of higher level performance management information including the development of key performance measures/indicators for assessing how well departments are managing their obligations in relation to critical infrastructure protection.

. . . . page 54

An essential component of devolved policy implementation is a system of internal accountability which includes a methodology or framework enabling implementation to be monitored to assess the extent to which policy objectives are being successfully achieved and to highlight any "problem" areas and allow for continuous review and improvement.

. . . . page 55

Greater attention needs to be given to developing a more formalised structure of performance evaluation in relation to monitoring, measuring and reporting on how well:

- operators/owners of critical infrastructure and essential services are fulfilling their critical infrastructure protection obligations;
- relevant departments/agencies (including Victoria Police) are performing their legislative and policy responsibilities; and
- the Department of Premier and Cabinet is performing its strategic leadership and oversight role.

. . . . page 55

Recommendation 4:

The Committee recommends that the Department of Premier and Cabinet re-consider the Auditor-General's recommendation relating to the development of a performance measurement framework for critical infrastructure protection arrangements in Victoria. Consideration should be given to the development of relevant indicators which assess the extent to which the policy framework is being implemented across departments/agencies and highlighting any areas which may require investigation or attention.

. . . . .page 55

Recommendation 5:

The Committee recommends that the Department of Premier and Cabinet consider and identify key information and indicators to evaluate how well the Department is performing in terms of its own strategic leadership and oversight of critical infrastructure (including essential services) protection arrangements in the State of Victoria.

. . . . .page 55

Recommendation 6:

The Committee recommends that all government departments with responsibilities in relation to declared essential services under Part 6 of the *Terrorism (Community Protection) Act 2003* and with responsibilities for the protection of critical infrastructure in the State have appropriate systems in place to monitor and report on their own management performance, to assist proper accountability and identify and drive improvement where needed.

. . . . .page 56

Recommendation 7:

The Committee recommends that Victoria Police develop a more formalised internal management reporting system which enables an assessment to be made of their performance in relation to their training exercise supervisory responsibilities under Part 6 of the *Terrorism (Community Protection) Act 2003* and also in relation to their responsibilities under the *Victorian Framework for Critical Infrastructure Protection from Terrorism*, and any subsequent iteration of the policy.

. . . . .page 56

Section 4.4.3 – Clarification of roles and responsibilities

The Department of Premier and Cabinet intends that a revised CIP policy Framework will more clearly define policy objectives and accurately describe the roles and responsibilities of government departments and industry users. Also government departments will be consulted to develop an agreed view about their roles and responsibilities in the new Framework.

. . . . .page 59

It is evident that there are a number of "best practice" models for the management and oversight of the protection of the State's essential services and critical infrastructure within the Victorian public sector which could be adapted and applied across other government departments with similar responsibilities.

. . . . .page 59

Recommendation 8:

The Committee recommends that the Department of Premier and Cabinet and Victoria Police:

(a) Take action to identify examples of "best practice" (benchmarks) in relation to the management of departmental responsibilities relating to the protection of essential services under Part 6 of the *Terrorism (Community Protection) Act 2003* and the protection of the Victoria's critical infrastructure; and

(b) Disseminate these "best practice" models to other government departments with critical infrastructure responsibilities to assist with the improvement of critical infrastructure protection management systems and processes across the public sector.

. . . . .page 60

Section 4.4.4 – Guidance on identification of essential services for declaration under the Act

Under Part 6 of the Act, the Premier designates responsibility for the application of the Section to "relevant Ministers" who may then delegate their powers to a "relevant public service officer". The Department of Premier and Cabinet do not track those delegations but intends to formalise the process across "relevant departments" in the future.

. . . . .page 60

Recommendation 9:

The Committee recommends that the Department of Premier and Cabinet proceed with its intention to formalise and standardise the delegation process by relevant departments under Section 27A of Part 6 of the *Terrorism (Community Protection) Act 2003* to ensure that departments adopt a common process for ensuring delegates are fully aware of their powers and functions under the Act and that a process is in place to regularly review delegations to ensure they remain relevant and appropriate.

. . . . .page 63

Section 4.4.5 – Inter-agency risk management

Under the *Victorian Risk Management Framework*, the Department of Premier and Cabinet has a pivotal role in state-wide risk management through coordination of the Cabinet process and support of the Premier on government-wide issues, as well as in his portfolio of ministerial responsibilities.

. . . . .page 66

As administrator of Part 6 of the Act and the agency responsible for the oversight of critical infrastructure protection policy in the State, the Department of Premier and Cabinet has an important role to play in ensuring that inter-agency risks associated with the application and implementation of critical infrastructure protection legislation and policy have been identified and are considered as part of the Department's risk management planning processes. Another important component of the Department of Premier and Cabinet's critical infrastructure risk management strategy is the identification and consideration of management risks which may have an impact on the effective implementation of policy objectives and legislative requirements.

. . . . .page 67

Recommendation 10:

The Committee recommends that the Department of Premier and Cabinet ensure that inter-agency and state-wide risks associated with the implementation of critical infrastructure protection arrangements in the State are identified as a part of the Department's risk management planning processes and that appropriate strategies are developed to manage those risks.

. . . . . . .pages 67

Recommendation 11:

The Committee recommends that the Department of Premier and Cabinet's risk management approach, in relation to its central oversight of critical infrastructure arrangements, takes into consideration any risks associated with: poor central oversight and direction; lack of appropriate and relevant performance measurement; and informal and unstructured reporting systems; together with strategies to address those risks.

. . . . .page 67

Section 4.4.6 – The Security and Continuity Network structure

Security and Continuity Networks in the transport, water and energy sectors are well established and appear to be operating effectively as intended.

. . . . .page 72

There has been a lack of commitment on the part of the Department of Health, the Department of Human Services and the Department of Business and Innovation in supporting the State's CIP policy Framework and local industry groups within their portfolios.

. . . . .page 72

The Security and Continuity Network-Coordination Group and the Department of Health have been remiss in ensuring the identification of critical infrastructure in the health sector.

. . . . pages 73

Recommendation 12:

The Committee recommends that the Department of Health make it a priority to identify a complete list of Victoria's health sector critical infrastructure and take action to ensure that procedures are in place to protect this infrastructure from all identifiable threats and risks.

. . . . page 73

Recommendation 13:

The Committee recommends that the Security and Continuity Network-Coordination Group take action to ensure that all critical infrastructure sites in the Victorian health sector are identified and that appropriate risk management strategies are in place to protect those sites.

. . . . page 73

Recommendation 14:

The Committee recommends that the Security and Continuity Network-Coordination Group take action to include the Department of Health in discussion and sharing of information to assist in the security and risk management protection of critical infrastructure sites in the health sector.

. . . . page 73

Section 4.4.7 – Effectiveness of the Security and Continuity Network-Coordination Group

The Security and Continuity Network-Coordination Group has not been proactive or diligent in performing its responsibilities in the past. As such, the effectiveness of the Group since its inception in April 2007 has been less than satisfactory.

. . . . page 75

The Department of Premier and Cabinet considers that the Security and Continuity Network-Coordination Group may not be the most appropriate forum for monitoring the application of Part 6 of the Act or for providing leadership in the management of risks relating to critical infrastructure in the State in the future.

. . . . page 76

Significant action is needed to improve the effectiveness of the Security and Continuity Network-Coordination Group particularly in relation to its guidance and monitoring responsibilities.

. . . . page 76

Recommendation 15:

The Committee recommends that the Security Continuity Network-Coordination Group should be more diligent in carrying out its responsibilities with regard to ensuring that the Security and Continuity Networks are operating effectively and as intended and that the Auditor-General review its diligience and effectiveness over the next two years.

. . . . .page 76

Recommendation 16:

The Committee recommends that the Security Continuity Network-Coordination Group seek to identify "best practice" Security and Continuity Networks in an effort to highlight practices and activities which might be adopted in those less well developed Networks.

. . . . .page 76

Section 4.4.8 – Role of the Central Government Response Committee in the Security and Continuity Network structure

The Department of Premier and Cabinet plans to strengthen the reporting arrangements between the Security and Continuity Network-Coordination Group and the Central Government Response Committee.

. . . . .page 78

Strengthening and formalising the reporting arrangements between the Security and Continuity Networks and the Security and Continuity Network-Coordination Group should provide benefits in terms of the quality of reporting from the Security and Continuity Network-Coordination Group to the Central Government Response Committee.

. . . . .page 78

Recommendation 17:

The Committee recommends that the reporting arrangements in place between the Security and Continuity Networks and the Security Continuity Network-Coordination Group be improved to provide more regular and standardised reports on the status of the key issues relating to the protection of critical infrastructure in the State such as: the identification and recording of sites; the status of risk management arrangements and business continuity planning; and emergency training.

. . . . .page 78

CHAPTER 5 – RISK MANAGEMENT AND COMPLIANCE

Section 5.2 – Identifying essential services and critical infrastructure

The proper identification of critical infrastructure is very important in ensuring that risk management plans are prepared to protect the assets and services from risks or threats and to mitigate the impact of these threats should they eventuate.

. . . . .page 86

The current CIP arrangements in Victoria, have led to a "dual system" of management whereby there is a need to identify critical infrastructure under the CIP policy Framework and a further "classification" process is required to identify essential services for the purposes of the statutory requirements under Part 6 of the Act (i.e. a set of mandatory requirements and a set of voluntary good practice principles). This has created some confusion amongst government and industry stakeholders.

. . . . .page 86

Work has been undertaken by the Department of Premier and Cabinet and Victoria Police with assistance from the VMIA, to develop the *Victorian Critical Infrastructure Classification Framework* which will assist in identifying critical infrastructure and determining what makes critical infrastructure a "declared essential service" for the purposes of the Act.

. . . . .page 87

The newly developed tool for applying the new Classification Framework is in the early stages of being rolled out by Victoria Police and is a sizable task with a rough assessment provided of around 18 months to complete the review of the current critical infrastructure register.

. . . . .page 87

Recommendation 18:

The Committee recommends that the Department of Premier and Cabinet and Victoria Police establish target dates for the implementation of both the *Victorian Infrastructure Classification Framework* and the methodology to determine declared essential services and report this timetable, together with regular progress updates, to the Security and Continuity Network-Coordination Group for approval and monitoring. The project timelines and progress updates should also be provided to the Central Government Response Committee for noting.

. . . . .page 87

The terms critical infrastructure and essential services continue to be used interchangeably.

. . . . .page 88

The management of critical infrastructure and essential services protection in the State is in need of simplification. The existence of legislation for risk management in respect to the threat of a terrorist incident affecting declared essential services and a separate policy encouraging compliance of owners/operators of critical infrastructure represents unnecessary and confusing layers of direction and administration.

. . . . .page 88

National guidelines identify five levels of criticality for the identification and prioritisation of critical infrastructure. These have been adopted in the development of the *Victorian Critical Infrastructure Classification Framework*.

. . . . .page 89

There are degrees or levels of "criticality" which Victoria Police consider when prioritising sites in terms of their importance from a risk management perspective.

. . . . .page 89

Recommendation 19:

The Committee recommends that as part of its revision of the *Victorian Framework for Critical Infrastructure Protection from Terrorism*, the Department of Premier and Cabinet develop a more comprehensive, all encompassing policy framework which specifies relevant and appropriate criteria for determining levels of criticality for the State's critical infrastructure together with specific management regimes applicable to each category and an appropriate reporting framework to improve assurance and accountability over the State's critical infrastructure protection arrangements.

. . . . .page 90

Section 5.3 – Risk management

Overarching risk management in both the public and private sector is the international risk management standard ISO 31000:2009 "*Risk Management – Principles and guidelines*" which promotes the implementation of a risk management framework incorporating an integrated approach to the management of all types of risk.

. . . . .page 90

The *Victorian Government Risk Management Framework* issued by the Department of Treasury and Finance takes account of the principles and guidelines set out in ISO 31000:2009. As a minimum, the revised Framework calls for Victorian public sector agencies to risk manage their operations consistent with AS/NZS ISO 31000:2009, the directions issued under the *Financial Management Act 1994* and with the principles outlined in the *Victorian Government Risk Management Framework* itself.

. . . . .page 91

The CIP policy Framework and the National Counter Terrorism Committee's critical infrastructure protection guidelines also refer to the Risk Management Standards.

. . . . .page 91

There are a range of existing policies, manuals, regulations and codes relating to emergency management, safety management and risk management mitigation in the State such as: dangerous goods regulations; occupational health and safety regulations; gas and electricity regulations and safety codes; food safety regulations; immunisation programs; warning systems; and community education and awareness programs.

. . . . . pages 92-5

Section 5.4 – Auditor-General's review of the audit and validation of critical infrastructure risk management plans

Victoria Police have a clear role to play under Part 6 of the Act in relation to supervising exercises to test the adequacy of risk management plans of declared essential service operators in regard to the threat of a terrorist incident. Evidence taken at the hearing suggested that Victoria Police had been diligent in performing its obligations under the Act.

. . . . page 97

Under the CIP policy Framework, Victoria Police is required to assist owners/operators of critical infrastructure in their development, validation and audit of risk management plans.

. . . . page 97

There are no compulsory requirements for the owners/operators of critical infrastructure to develop risk management and business continuity plans and Victoria Police only attend exercises and/or provide comments or advice to owners/operators as requested.

. . . . page 98

Section 5.4.5 – Definitions and terminology relating to critical infrastructure protection risk management

It is eight years since the Act came into operation and four years since the CIP policy Framework was released. The Department of Premier and Cabinet has been slow to take steps to clarify the definitions and terminology used in the policy and legislation to assist interpretation and consistent and appropriate compliance by Victoria Police, the relevant government departments and the owners/operators of critical infrastructure and declared essential services.

. . . . page 99

The Department of Premier and Cabinet needs to ensure that concepts and definitions in relation to the preparation of risk management plans and the testing of those plans are clearly and consistently defined in any revised CIP policy framework to limit any confusion and assist in ensuring obligations are consistently understood and satisfactorily met.

. . . . page 99

A working group has been established, led by Victoria Police, to develop guidance notes to establish a common understanding of the requirements of Part 6 of the Act. However, there is also a need for the Department of Premier and Cabinet to clarify the policy obligations of departments/agencies under the current CIP policy Framework in respect to the risk management of critical infrastructure within their portfolios.

. . . . page 99

Recommendation 20:

The Committee recommends that the Department of Premier and Cabinet ensure that any revised critical infrastructure protection policy for the State includes clearly defined and agreed terminology in relation to the preparation, audit and testing of risk management plans to limit confusion and inconsistency and to assist stakeholders in the effective application of the *Terrorism (Community Protection) Act 2003* and associated policy.

. . . . . . .page 100

Section 5.4.6 – Critical infrastructure risk management obligations of departments/agencies

Relevant departments and agencies have a range of risk management obligations under the CIP policy framework and under Part 6 of the Act. It is imperative that departments have adequate processes in place to monitor and support compliance in relation to these obligations within their industry sectors.

. . . . . . .page 100

Recommendation 21:

The Committee recommends that all departments/agencies with key roles and responsibilities in relation to the support of critical infrastructure protection have appropriate processes and systems in place to ensure they are meeting their obligations under both Part 6 of the *Terrorism (Community Protection) Act 2003* and the current *Victorian Framework for Critical Infrastructure Protection from Terrorism*.

. . . . . . .page 101

Recommendation 22:

The Committee recommends that the Security and Continuity Network-Coordination Group review the critical infrastructure risk management monitoring and reporting arrangements established by relevant departments in an effort to identify examples of best practice which can be used to assist improvement in other departments/ agencies.

. . . . . . .page 101

Section 5.4.7 – Critical infrastructure risk management for all hazards

Public policy and legislation must be responsive to changes and developments in the operating environment in order to remain relevant and effective.

. . . . . . .page 101

There has been a shift in emphasis at the national level, which has been adopted by the Council of Australian Governments (COAG), in relation to disaster management preparedness and response and critical infrastructure protection. There have also been a number of incidents in recent times, other than a terrorist attack, which have been caused by risks and threats which have manifested in Australia and internationally.

. . . . . . .page 101

The Department of Premier and Cabinet intend to address risks on an "all hazards approach" under a revised CIP policy Framework and to also recognise the concept of "building resilience" as adopted by COAG.

. . . . . . .page 101

Recommendation 23:

The Committee recommends that relevant departments/agencies with key roles and responsibilities in relation to the support of critical infrastructure protection implement actions to promote and encourage an all hazards approach to risk management by owners/operators of critical infrastructure and essential services within their portfolios to ensure that strategies have been developed to prepare for the possible occurrence of a range of security risks and threats.

. . . . . . .page 102

Section 5.4.8 – Risk management compliance by critical infrastructure owners/operators

There is no way of comprehensively assessing the level of satisfactory compliance by industry owners/operators of critical infrastructure and essential services with the risk management provisions outlined in the CIP policy Framework.

. . . . . . .page 102

Some information is available through Victoria Police of compliance by declared essential services operators with the terrorist risk management training exercises required under Part 6 of the Act.

. . . . . . .page 102

There are a whole suite of standards, legislation and regulations outlining risk management requirements and providing good guidance on risk management principles for both the private and public sectors.

. . . . . . .page 102

These overlapping strategies and regulations need to be taken into account as part of the forthcoming review of the *Terrorism (Community Protection) Act 2003* and in particular in regard to whether the mandatory risk management provisions outlined in Part 6 of the Act are adding value or whether there is a more efficient way of proceeding.

. . . . . . .page 103

Existing industry legislation, regulations and contract/licensing arrangements between the State of Victoria and the owner/operator, may provide a range of options which could be explored as a method of obtaining some level of assurance by way of certification or declaration by the owners/operators of critical infrastructure and essential services, that adequate risk management plans have been prepared in accordance with ISO 31000:2009 and/or with other national or state policy.

. . . . . . .page 103

Recommendation 24:

The Committee recommends that the Department of Premier and Cabinet investigate avenues available through existing industry legislation, regulations or contract/licensing agreements for industry owners/operators to provide some certification or assurance that they, the owners/operators of critical infrastructure and essential services, are taking appropriate action to protect Victoria's critical infrastructure and essential services from a range of identified risks and hazards.

. . . . . . .page 103

Section 5.5 – Training exercises and continuous improvement

The State Exercise Steering Committee is a sub-committee of the State Multi-Agency Emergency Management Training and Exercising Strategy Committee within the Office of the Emergency Services Commissioner and its purpose is to develop a multi-agency emergency management exercise strategy and oversee the implementation of development exercise programs in line with strategic operational direction provided by EMTESC.

. . . . . . .page 105

Victoria Police monitors the lessons learned from its assessment of training exercises to assist continuous improvement in the area. The sharing of knowledge and awareness of critical infrastructure and declared essential services issues between various government departments has been the subject of an ongoing program.

. . . . . . .page 106

Exercise feedback reporting, compliance letters and debriefs undertaken by Victoria Police as part of their responsibilities in assessing training exercises under Part 6 of the Act have now all been standardised.

. . . . . . .page 106

Victoria Police retains centralised hard copy files on all declared essential services owner/operators containing information relating to their Part 6 annual training exercise. The industry operators and relevant departments also retain this information as part of their responsibility for undertaking training exercises under Part 6 of the Act.

. . . . . . .page 106

With regard to Part 6 exercises, Victoria Police oversee 39 exercises each year and have only had one occasion where an operator has failed a test.

. . . . . . .page 107

An extensive amount of work has been undertaken through the Victorian Emergency Management Council in the last few years to ensure appropriate multi-agency training is occurring and regularly reported upon in terms of improvement. Since 2009 there has been substantial investment by the State Government in emergency management largely as a result of the 2009 bushfires and more recently floods in the State.

. . . . page 108

Whilst this investment has not been directly attributed to counter-terrorism, it is anticipated that much of the enhancements to capability and infrastructure will ultimately benefit the emergency sector should it be required to respond to a terrorist incident.

. . . . page 108

The Auditor-General's audit did not include any review of the State's emergency management arrangements. The Auditor-General's review focussed on "preparedness to respond" to a terrorist incident and not the response after an incident. However, emergency preparedness and emergency response are closely linked.

. . . . page 110

In terms of testing the level of preparedness of operators of declared essential services to a terrorist incident, Victoria Police has sought to perform its responsibilities under Part 6 of the Act, diligently and professionally.

. . . . page 111

The level of preparedness in relation to the operators of critical infrastructure sites, not covered by the provisions of Part 6, is less easy to assess as the information appears to be spread across a number of relevant departments who, according to the Auditor-General, have systems and procedures of varying quality in place to monitor and oversee the risk management plans and emergency preparedness of these operators.

. . . . page 111

There could be advantages in making greater use of the specialised emergency preparedness training arrangements within the Office of the Emergency Services Commissioner in:

- assisting owners/operators of critical infrastructure with their general emergency preparedness; and
- providing a central database of critical infrastructure protection exercises for analysis and diseemination.

. . . . pages 111-2

The Department of Justice indicated that with the OESC moving towards a regulator and inspectorate model, it would be appropriate for the agency to have a role testing the emergency preparedness of owners/operators. Such a role would not be envisaged to replace the existing regime of relevant departmental responsibilities but could provide independent assessment and expertise to drive improvement in emergency preparedness.

. . . . page 112

Recommendation 25:

The Committee recommends that the Department of Premier and Cabinet together with the Department of Justice consider utilising the expertise of the Office of the Emergency Services Commissioner in developing and conducting training exercises to assist owners/ operators of critical infrastructure and essential services in validating their emergency management planning and preparedness to a range of risks/threats.

. . . . page 112

Recommendation 26:

The Committee recommends that Department of Premier and Cabinet together with the Department of Justice consider the option of the Office of the Emergency Services Commissioner providing a centralised database of critical infrastructure protection training exercises to enable central analysis to better identify and share improvement strategies.

. . . . page 112

CHAPTER 1: BACKGROUND TO THE INQUIRY

1.1 Introduction

Under Section 14 of the *Parliamentary Committees Act 2003*, the Committee is able to inquire into, consider and report to the Parliament on any proposal, matter or thing concerned with public sector administration.[1]

In accord with this Section of the Act, the Committee conducts reviews to assess the status of actions taken by public sector departments and agencies to address issues identified and recommendations made in Auditor-General's performance audit reports and to make further recommendations for improvement where necessary.

The Committee applies a set of criteria in order to identify those audit reports considered to be the highest priority for Committee review and follow-up.

The findings of the January 2009 Auditor-General's report *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure* were identified by the Committee as significant in terms of public interest and importance to the State and therefore selected for detailed follow-up inquiry by the Committee.

1.2 Objective and scope of the Auditor-General's report: *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*

The objective of the audit was to examine the State's preparedness to respond to terrorism incidents relating to essential services and critical infrastructure. The principal agencies examined were the Department of Premier and Cabinet and Victoria Police. The audit also included a review of the activities of six departments with roles and responsibilities under the *Terrorism (Community Protection) Act 2003* (the Act) and the *Victorian Framework for Critical Infrastructure Protection from Terrorism* (CIP policy Framework).[2]

Specifically, the audit examined whether:[3]

- there was a clear governance structure in place, specifying the roles, responsibilities and accountabilities of public sector agencies;
- inter-agency risks had been identified and were being managed effectively;
- effective consultation and communication between public sector agencies and owner/operators occurred;
- the progress of implementation of the Act and the CIP policy Framework was being monitored; and

[1] *Parliamentary Committees Act 2003,* s. 14(a)(i)

[2] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, pp.18-19

[3] ibid., p.3

- arrangements were in place within the responsible agencies to monitor the preparedness and capability of owners/operators to respond to terrorist incidents.

The audit also considered the amount of funding which had been provided for counter-terrorism initiatives including for prevention, response and recovery from terrorist attacks.

1.3 Overall conclusions and recommendations of the Auditor-General

The Auditor-General noted that Victoria had been the first Australian jurisdiction to develop arrangements for protecting essential services from terrorist incidents and had been instrumental in developing capability for protecting essential services and critical infrastructure both nationally and in other states and territories.[4]

Overall, the Auditor-General considered that most elements of the State's preparedness to respond to terrorism incidents were satisfactory however there were some aspects which required improvement.[5]

The Auditor-General acknowledged in his report the advice from the Department of Premier and Cabinet (DPC) that the Department intended to undertake a review of Victoria's critical infrastructure protection arrangements, including Part 6 of the Act and the CIP policy Framework.[6]

A more detailed overview of the Auditor-General's recommendations is contained in Chapter Three of this report.

1.4 Responses of audited agencies

Responses from the DPC, Victoria Police and each of the six "lead departments" audited were included in the Auditor-General's report.

The responses published in the Auditor-General's report were mostly supportive with the exception of some differences in opinion between the DPC and the Auditor-General concerning the role of the Department in terms of oversight and monitoring. For the main part, the DPC responded to the Auditor-General that:[7]

> *The Department of Premier and Cabinet 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.*

[4] ibid., p.4

[5] ibid., p.12

[6] ibid., p.6

[7] ibid., p.11

1.5 Other recent audits related to risk management and critical infrastructure protection

In recent years, the Auditor-General has tabled reports dealing with similar issues to those raised in his report on the protection of essential services and critical infrastructure. These are:

- *Bio-security Incidents: Planning and Risk Management for Livestock Diseases* (November 2008). This audit reviewed the effectiveness of the planning and risk management arrangements in place to manage bio-security risks to Victoria's livestock industry. The report was the subject of a follow up inquiry by the Public Accounts and Estimates Committee (PAEC) in September 2010; and

- *Security of Infrastructure Control Systems for Water and Transport* (October 2010). This audit assessed the security of systems used to operate, manage and control water and transport infrastructure.

The findings in the October 2010 report are particularly pertinent to the Committee's inquiry as they relate to the security of the systems (such as "Supervisory Control and Data Acquisition" (SCADA) systems) used in the water and transport industries to control and manage infrastructure such as, power grids, dams, water treatment and distribution facilities, and tram/train power and signalling systems. In this report, the Auditor-General concluded that:[8]

> *Operator control systems for critical infrastructure are not secure. As a result, the ongoing delivery of essential water and transport services is at risk.*

And also:[9]

> *Portfolio agencies have not effectively monitored and supported operators to manage their infrastructure control systems risks. As a result, the emerging information and communication technology (ICT) risks and vulnerabilities facing the State's essential services have not been identified and prioritised for attention.*

1.6 Scope of the review undertaken by the Committee

On 30 May 2011, Mr Des Pearson, Auditor-General, provided the Committee with a briefing on the issues identified during the audit and his views about which issues were of greatest significance.

The Committee held a public hearing on 25 August 2011 with representatives from the Victorian Auditor-General's Office, the Department of Premier and Cabinet, the Department of Justice and Victoria Police. The purpose of the hearing was to discuss the matters raised in the report and obtain information on actions undertaken since the tabling of the audit report in January 2009 and the *Response by the Minister for Finance to the Auditor-General's Reports 2008-09* tabled in December 2009.

[8] Victorian Auditor-General's Office, *Security of Infrastructure Control Systems for Water and Transport*, October 2010, p.5

[9] ibid., p.23

The public hearing was divided into five sessions as follows:

- Session 1: Introductory comments by the Auditor-General;
- Session 2: Representatives from the Department of Premier and Cabinet;
- Session 3: Representatives from the Department of Justice (including Victoria Police and the Office of the Emergency Services Commissioner);
- Session 4: Representatives from both the Departments of Premier and Cabinet and Justice (joint session); and
- Session 5: Concluding comments by the Auditor-General.

The Auditor-General and his representatives were present during each of the five sessions.

Following the public hearing, further information was requested in writing from the departments in relation to questions taken on notice at the hearings and any other additional material required by the Committee.

The Committee's comments and conclusions are based on transcripts of evidence taken at the public hearing, written advice provided by the departments and the Auditor-General, and other relevant research.

1.6.1 Funding for counter-terrorism initiatives

The Auditor-General's report included a chapter on funding for terrorist preparedness however no specific issues were identified nor recommendations made. The Auditor-General noted some difficulty in quantifying the expenditure related solely to this area of activity. The report indicated that between October 2002 and June 2009, around $255 million had been allocated to counter-terrorist arrangements and activities across Victoria.

The Department of Premier and Cabinet advised the Committee that since 2008, funding for counter-terrorism arrangements have been absorbed into the general budget of the Commonwealth and state and territory governments, rather than appearing as a separate line item.[10]

The Department of Justice advised that between June 2009 and June 2012, further general emergency services funding totalling $474.8 million has been allocated for initiatives in the Department's emergency services area and Victoria Police which, while not specifically related to counter-terrorism preparedness, provide assets and services which would be called on in the event of a terrorist emergency incident.[11]

Funding matters relating to the protection of essential services and critical infrastructure from terrorism is beyond the scope of the Committee's current Inquiry. The Committee notes the difficulties reported by the Auditor-General in isolating this funding and looks forward to possible future reports which identify the funding provided for counter-terrorism preparedness activities and seek to assess the effectiveness of this funding.

[10] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.16

[11] Ms P. Armytage, Secretary, Department of Justice, letter to the Committee, received 15 June 2011, p.5

Recommendation 1:

The Committee recommends that, to enhance transparency, the Department of Treasury and Finance consider issuing Financial Reporting Directions requiring all departments and agencies to identify and report within their Annual Reports funding allocated for counter-terrorism initiatives and activities, such as preparedness training, risk management and support to industry and other relevant stakeholders.

CHAPTER 2: CONTEXT – CRITICAL INFRASTRUCTURE PROTECTION IN AUSTRALIA

2.1 What is critical infrastructure?

Critical infrastructure is a term used by governments to describe assets which are essential to the functioning of a society and an economy. Critical infrastructure extends across many sectors of the economy including banking and finance, transport and freight, energy, water, communications, health and food supply. Some elements in these sectors are not strictly "infrastructure" but may be networks or supply chains that support the delivery of essential products or services.

The following list provides an indication of those facilities most commonly associated with the term "critical infrastructure":

- electricity generation, transmission and distribution;
- gas production, transport and distribution;
- oil and oil products production, transport and distribution;
- telecommunications;
- water supply (drinking water, waste water/sewerage);
- agriculture, food production and distribution;
- heating (natural gas, fuel, oil);
- public health (hospitals, ambulances);
- transportation systems (fuel supply, rail network, airports, harbours, inland shipping);
- financial services (banking, clearing); and
- security services (police, military).

The Australian Government defines critical infrastructure as:[12]

> *…those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.*

[12] Australian Government, Trusted Information Sharing Network, *Critical Infrastructure Protection National Strategy*, 12 March 2004, p.3

2.2 What is critical infrastructure protection?

Critical infrastructure can be damaged, destroyed or disrupted by mechanical breakdowns, negligence, natural disasters, accidents, illegal criminal activity and/or malicious damage. As such, it is the aim of government policy and owners/operators of critical infrastructure to take action to protect assets and the supply of services against these potential threats and weaknesses through improved security and the development of safeguards and risk mitigation strategies.

The interdependency of critical infrastructure sectors mean that a disruption in one sector can lead to impacts in another sector, for example, a virus that disrupts gas distribution could lead to a consequential reduction in electrical power generation which could in turn lead to a shutdown of computerised networks and communications systems in other sectors. A recent example of this interdependency in Victoria occurred during the Black Saturday bushfires in February 2009 when electrical outages affected reticulated water supply systems, dependent upon mains power, and some water treatment plants.[13]

The degree and complexity of these interdependencies is increasing as society becomes more reliant on shared information systems and convergent technologies, including the Internet. Advances in technology have seen systems which were once physically and logically independent and separate become more automated, interdependent and interrelated and hence more vulnerable to widespread physical and cyber disruption.

The community has an expectation that services such as water and power will be available as needed and that they will be provided in a reliable and safe manner. With society's increasing reliance on these services comes the increasing importance of effective protection of the infrastructure by governments and private owners and operators.

Critical Infrastructure Protection (CIP) provides the link between risk management and infrastructure assurance. It is not a new discipline but rather brings together a number of pre-existing specialisations which deal with the prevention, preparedness, response and recovery arrangements for disasters and emergencies, including:[14]

- law enforcement and crime prevention;
- emergency management;
- risk management;
- business continuity planning;
- national security and defence;
- counter terrorism;
- protective security;
- natural disaster planning and preparedness;

[13] B. Anderson, Goulburn Valley Water, *Lessons from the 'Black Saturday' Fires,* paper presented at 72nd Annual Water Industry Engineers and Operators' Conference, Bendigo, September 2009, pp.106, 110

[14] Australian Government, Trusted Information Sharing Network, *Critical Infrastructure Protection National Strategy*, 12 March 2004, p.4

- e-security; and
- market regulation, planning and infrastructure development.

Because a large proportion of Australia's critical infrastructure is owned/operated by the private sector, it is of utmost importance that industry and government work together to raise awareness of the importance of managing critical infrastructure and of the necessary elements to implementing an effective CIP policy Framework.

2.3 The risk environment

It should be noted that the risk environment can alter and correspondingly our focus and attention on preparing ourselves against particular risks alters also. Following the September 2001 terrorist attacks in the United States, terrorism attained a new prominence in the national security risk environment. The Bali bombings in October 2002 and 2005 and the attack on the Australian embassy in Jakarta in 2004 brought the threat of terrorism even closer to home. These attacks prompted Australian governments to review and enhance the country's counter-terrorism capabilities and arrangements.

The attention of Commonwealth and state and territory government legislation and policy was firmly focused on preparing against terrorism as a key risk and this flowed into policies relating to the protection of the nation's critical infrastructure.

In Australia, in recent times, natural disasters have taken on a new significance and demanded our attention as a direct result of their realisation, most notably the catastrophic Victorian bushfires on Black Saturday and more recently, the devastating flood events in Queensland and also in parts of Victoria during December 2010 and January 2011.

In addition to our recent focus on natural disasters, rapid developments in information technology and our increasing dependence on electronic systems which support our daily lives has seen the area of cyber security take on a greater prominence and the management of cyber risk become increasingly crucial and particularly pertinent to the protection of critical infrastructure systems.

The following extracts paint a picture of the risk and threat environment which government policy makers, public sector managers and private businesses in Victoria and Australia are dealing with:

> *"On Friday, September 25th, 1998, at about 12.26pm, a vessel ruptured at one of three gas plants operated by Esso at Longford, 20 kilometers from Sale, to process product flowing from wells in Bass Strait. The rupture led to the release of vapours and liquid. Several major explosions and fires followed. Two Esso employees, Peter Bubeck Wilson and John Francis Lowery, were killed. Eight others at the site were injured. Fires and leaks continued at the plant until the last fires were extinguished at 5.30pm on Sunday, September 27th (Royal Commission 1999; EMA 2004).*
>
> *As a result of the fires and explosions, all three gas plants were shut down. This led to an immediate cessation of processing of natural gas, liquid petroleum gas and crude oil. Supplies to all domestic, commercial and industrial consumers in metropolitan Melbourne and in several country areas were rapidly curtailed. Within 36 hours, all Victorian gas consumers had been instructed to turn off gas supply lines to homes and commercial premises.*

> *Gas company and emergency service personnel were mobilized to ensure the shut down was implemented.*
>
> *With the Longford facility supplying 98 per cent of the State's gas needs, most Victorian gas consumers were left without gas for 19 days."*[15]

> *"National Terrorism Public Alert System*
>
> *Australia is at MEDIUM level of alert. Australia has been at a 'medium' level of alert since the four levels of national terrorism alert were introduced in 2003…medium - terrorist attack could occur."*[16]

> *"A man had undertaken some contract work with an Australian firm that installed SCADA (Supervisory Control and Data Acquisition) radio-controlled sewage equipment for the Maroochy Shire Council. After he was unsuccessful in gaining subsequent employment with the Council he packed his car with stolen radio equipment attached to a computer and drove around the area on a least 46 occasions between February and April 2000 issuing radio commands to the sewage equipment he probably helped install. His actions caused 800,000 litres of raw sewage to spill into local parks, rivers and even the grounds of the Hyatt Regency Hotel."*[17]

> *"While terrorism has made the world more security conscious, governments and the private sector have been slow to realise how vulnerable they are to attacks on information systems…A recent Victorian Auditor-General's examination of Internet security management by four state government agencies found a wide range of problems, including lack of threat and risk analysis, poor procedures for handling security incidents, inadequate disaster recovery plans and weaknesses in anti-virus strategies."*[18]

> *"…attacks on public transport in Madrid (March 2004), London (July 2005) and Mumbai (July 2006 and November 2008) have highlighted the intent and capacity of terrorists to attack vulnerable surface transport systems. These systems include trains, buses, ferries and their terminals and exchanges… Queensland has introduced the Transport Security (Counter-Terrorism) Act 2008 which implements a system for identifying surface transport operations at an elevated risk of a terrorist attack and ensures they conduct*

[15] R. Walker, *Emergency management risk communication project — final report to the Department of Human Services — Appendix 1*, January 2006, p.1

[16] Australian Government, 'National Terrorism Public Alert System', <http://www.ema.gov.au/agd/WWW/NationalSecurity.nsf/Page/Information_for_Individuals_National_Security_Alert_System_National_Counter-Terrorism_Alert_System/>, accessed 10 October 2011

[17] M. Abrams, J. Weiss, *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia,* July 2008, p.1

[18] G. Hughes, *The Age*, 'The cyberspace invaders', 22 June 2003, <www.theage.com.au/articles/2003/06/21/1056119529509.html>, accessed 30 November 2011

risk assessments, develop security plans and implement and review security measures."[19]

The Victorian Auditor-General issued a report critical of the security of SCADA systems for the State's water and transport. The audit found that the risk of unauthorised access to water and transport infrastructure control systems is high and that security processes and controls were not satisfactory.[20]

"An unemployed truck driver has been accused of hacking into one of the service providers for the National Broadband Network and had control of its system for six weeks. The Australian Federal police allege that the hacking could have caused considerable damage to Australia's infrastructure. It is alleged the man is a self-taught hacker who acted alone, spending up to 20 hours per day on a home computer. It is alleged he was also responsible for an intrusion into Sydney University's computer system and had attempted to hack into other major companies."[21]

"The Minister for Health and Ageing, Nicola Roxon has announced that Australia's Pandemic Phase moves from PROTECT to ALERT signifying the end of the H1N1 influenza (swine flu) pandemic in Australia."[22]

"The number of fire starts involving electricity assets remains unacceptably high – at more than 200 a year. Although it is not possible to eliminate the risk posed by electricity assets, the State and the distribution businesses should take the opportunity to invest in improved infrastructure and substantially remove one of the primary causes of catastrophic fires in Victoria during the past 40 years."[23]

"The Victorian Managed Insurance Agency insures community assets such as roads, parklands, schools and community infrastructure. The agency informed the Commission that the estimated total amount of claims for lost or damaged assets and infrastructure is $76.7 million."[24]

"A damning 2007 assessment of Melbourne City Loop's emergency infrastructure recommended major upgrades, including elevating walkways, because evacuation would be "very restricted"... Metro did not answer

[19] Queensland Government, Department of Transport and Main Roads, 'Transport Security (Counter-Terrorism) Act 2008', <http://www.tmr.qld.gov.au/~/media/de0f6424-e5a8-4d6d-9c24-8d5e77a6f6ae/transport_security_fact_sheet.pdf>, accessed 7 October 2011

[20] Victorian Auditor-General's Office, *Security of Infrastructure Control Systems for Water and Transport,* October 2010

[21] B. Packham, *The Australian*, 'Man accused of hacking into NBN provider is refused bail', 27 July 2011, <http://www.theaustralian.com.au/news/nation/hacker-accused-of-threat-to-national-broadband-network/story-e6frg6nf-1226102794463>, accessed 5 August 2011

[22] Australian Government, Trusted Information Sharing Network, 'Current Issues', <www.tisn.gov.au/Pages/Current_issues.aspx>, accessed 7 October 2011

[23] 2009 Victorian Bushfires Royal Commission, *Final Report — Summary*, July 2010, p.12

[24] 2009 Victorian Bushfires Royal Commission, *Final Report — Volume 1*, Appendix A, July 2010, p.344

> *questions about how long it would take to evacuate passengers in the event of a tunnel fire or terrorist incident."*[25]
>
> *"NSW flags tougher laws following Orica spills – the changes were announced following the publication of a report into Orica's Kooragang island chemical leak on August 8. The leak was the first in a series for Orica, and resulted in a spray of hexavalent chromium, or chromium 6, covering parts of Stockton. Both Orica and the NSW Government were strongly criticised for the leak, particularly for the delays in Orica and the Government's reporting of it. Orica reported the leak 16 hours after it happened."*[26]
>
> *"Sydney police say they have caught a man carrying a homemade bomb at a busy train station in the city's west overnight.*
>
> *Robert Day was stopped by officers who were at Lidcombe Railway Station for a drug detection operation just after 7:30pm (AEDT).*
>
> *Police say they found a pipe bomb which was live and unstable inside a glasses case."*[27]

2.4 National terrorism and critical infrastructure protection arrangements

Australia's preparedness to the threat of terrorism combines the creation of effective legislation and the collection of intelligence with national defence, law enforcement, aviation and maritime security, border control, protective security, preventative health measures, emergency response management, the protection of public and private infrastructure, planning and testing responses and improving national and international cooperation.[28]

2.4.1 National Counter-Terrorism Committee

The National Counter-Terrorism Committee (NCTC) was established in October 2002 through an inter-Governmental Agreement between the Commonwealth and state and territory governments. The *National Counter-Terrorism Plan* (NCTP) developed by this Committee, outlines: the legal and administrative framework and responsibilities surrounding national, state and territory jurisdictions; the prevention and preparedness framework; response arrangements; and recovery management.

Under the NCTP, state and territory governments are responsible for:[29]

[25] M. Fyfe and C. Lucas, *The Age*, 'City Loop safety fears', 22 September 2011, <www.theage.com.au/victoria/city-loop-safety-fears-20110921-1klbd.html>, accessed 30 November 2011

[26] A. Duffy, Australian Mining, 'NSW flags tougher laws following Orica spills', 7 October 2011, <www.miningaustralia.com.au/news/nsw-flags-tougher-laws-following-orica-spills>, accessed 7 October 2011

[27] ABC News, 'Pipe bomb arrest at Sydney train station', 10 November 2011, <www.abc.net.au/news/2011-11-10/pipe-bomb-arrest-at-sydney-train-station/3656544>, accessed 30 November 2011

[28] Australian Government, 'Australian National Security', <www.ag.gov.au/agd/www/nationalsecurity.nsf >, accessed 5 May 2011

[29] Commonwealth of Australia, National Counter-Terrorism Committee, *National Counter-Terrorism Plan,* September 2005 (plus amendments relating to the National Counter Terrorism Alert System introduced October 2008), pp.2:2-2:3

- maintaining counter-terrorism and related policies, legislation and plans within their jurisdictions;
- maintaining counter-terrorism and consequence management capabilities in a number of public sector departments and agencies;
- primary operational response to terrorist incidents within their jurisdictions;
- determining prevention strategies and operational responses to threats;
- seeking assistance from, or providing assistance to, other jurisdictions;
- declaring a National Terrorist Situation in the event of a terrorist incident or threat, if considered necessary; and
- contributing to the national strategy in the event of a National Terrorist Situation.

In December 2002, the Council of Australian Governments (COAG) endorsed the development by the NCTC of the *National Guidelines for Protecting Critical Infrastructure from Terrorism* which covers the identification of critical infrastructure, guidelines about threat/risk assessment, prevention and preparedness, and response and recovery. These Guidelines were re-issued in 2011.

2.4.2 Critical Infrastructure Protection National Strategy

As a significant proportion of Australia’s critical infrastructure is owned and operated by the private sector, in 2001, the Prime Minister established a Business-Government Task Force on Critical Infrastructure. This Task Force recommended the establishment of an information sharing network to foster the business-government partnership and in April 2003, the Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection was established.

The TISN for Critical Infrastructure Protection is comprised of a number of Infrastructure Assurance Advisory Groups each representing a different industry sector. These Groups provide a forum in which owners and operators of critical infrastructure and industry representatives work together and share information on threats, vulnerabilities and risk management solutions.

In 2004, the TISN for Critical Infrastructure Protection developed the *Critical Infrastructure Protection National Strategy* (the CIP National Strategy). This Strategy presents an overarching statement of principles for critical infrastructure protection in Australia, outlining the major tasks and assigning responsibilities necessary for their application to provide a common understanding among stakeholders.

In June 2010, the Australian Government released the *Critical Infrastructure Resilience Strategy* which seeks to build on the CIP National Strategy. This is discussed further in Section 2.6.1. At the national level, the term “critical infrastructure protection” is used only to describe actions or measures taken to mitigate against the threat of terrorism whilst “critical infrastructure resilience” takes an “all hazards” approach to critical infrastructure and encompasses prevention, preparedness, response and recovery for a range of risks and threats.[30] The Committee notes recent advice from the Department of Premier and Cabinet (DPC) that despite its title the current *Victorian Framework for Critical Infrastructure Protection from Terrorism* (CIP policy Framework) has been focused on managing risk from an "all hazards" perspective and that the concept of resilience will be incorporated into a revised CIP policy.[31]

2.5 Victorian Government security and safety

The DPC and Victoria Police are the two key government agencies with responsibilities for managing the State's preparedness to respond to the threat of terrorism. While prime responsibility for the protection of critical infrastructure and essential services rests with the owners/operators, these agencies also have a significant role in the oversight of critical infrastructure protection arrangements under state legislation and policy.

A number of portfolio departments also have responsibilities under State Government legislation and policy in relation to the protection of essential services and critical infrastructure from the threat of terrorism.

Also, the Department of Justice has key emergency management responsibilities and other responsibilities in relation to critical infrastructure protection.

2.5.1 State Government legislation relating to terrorism

There are two main pieces of legislation relevant to the preparation for, and response to, a terrorist incident in Victoria. These are the *Terrorism (Community Protection) Act 2003* and the *Emergency Management Act 2006*.

Terrorism (Community Protection) Act 2003

The *Terrorism (Community Protection) Act 2003* (the Act) provides powers and obligations relating to the prevention of, and response to, terrorist acts. It includes provisions relating to the issue of warrants, preventative detention orders, mandatory reporting of the loss or theft of certain chemicals, risk management by operators of certain essential services and the protection of counter-terrorism methods from disclosure during legal proceedings.

Part 6 of the Act specifically relates to essential services infrastructure risk management. The Premier of Victoria (through the DPC) is responsible for the administration of Part 6 of the Act. Part 6 of the Act defines an essential service as any of the following services:[32]

- transport;
- fuel (including gas);
- light;
- power;

[30] Attorney-General's Department, National Counter Terrorism Committee, *National Guidelines for Protecting Critical Infrastructure from Terrorism,* 2011, p.2

[31] Department of Premier and Cabinet, *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure,* June 2011, p.6

[32] *Terrorism (Community Protection) Act 2003*, s. 26

- water;
- sewerage; and
- any service, declared to be an essential service by the Governor-in-Council.

Emergency Management Act 1986

The *Emergency Management Act 1986* together with the *State Emergency Response Plan* and the *Emergency Management Manual Victoria*, establish roles and responsibilities and outline the organisational arrangements surrounding the planning and operational management for preparedness, response and recovery activities relating to emergency situations faced by the Victorian community, including any which may result from a terrorist incident.

Under the *Emergency Management Act 1986*, an emergency is defined as:[33]

> *…an event which in any way endangers or threatens to endanger the safety or health of any person in Victoria or which destroys or damages, or threatens to destroy or damage, any property in Victoria, or endangers or threatens to endanger the environment or an element of the environment in Victoria, including:*
>
> *(a) an earthquake, flood, wind-storm or other natural event; and*
>
> *(b) a fire; and*
>
> *(c) an explosion; and*
>
> *(d) a road accident or any other accident; and*
>
> *(e) a plague or an epidemic; and*
>
> *(f) a warlike act, whether directed at Victoria or part of Victoria or at any other state or territory of the Commonwealth; and*
>
> *(g) a hi-jack, siege or riot; and*
>
> *(h) a disruption to an essential service.*

Other State legislation and regulations

Legislation and regulations relating to security and safety issues in critical infrastructure and essential services industries are numerous and complex. For example, the transport, energy and water sectors of the Victorian economy are covered by legislation and regulations some of which contain provisions relating to:

- prohibited access to the land or premises where there is critical electricity infrastructure; and unauthorised interference with electricity infrastructure plant or equipment (*Electricity Industry Act 2000*);

[33] *Emergency Management Act 1986,* s. 4

- offences relating to interference with gas transmission infrastructure (*Gas Industry Act 2001*) ; and
- infrastructure risk management of sites and facilities from an occupational health and safety standpoint (e.g. *Electricity Industry Act 2000*; *Gas Industry Act 2001*; *Gas Safety Act 1997*; *Rail Safety Act and Regulations 2006*; etc).

Many of the regulations form part of the licensing requirements of the operators of transport, energy and water corporations.

In addition, Energy Safe Victoria (ESV) is the independent technical regulator responsible for electricity, gas and pipeline safety in Victoria. ESV has a broad role overseeing the design, construction and maintenance of electricity, gas and pipeline networks across the State through to ensuring that home electrical appliances meet certain safety and energy efficiency standards before they are sold.

There are also national bodies and guidelines which have been established with the agreement of state and territory governments and also legislation and regulations in other Australian jurisdictions (Commonwealth and state) relating to critical infrastructure and essential services which need to be considered by owners/operators especially where their infrastructure and/or services cross state borders.

2.5.2 State government critical infrastructure protection policy

The *Victorian Framework for Critical Infrastructure Protection from Terrorism*, released in April 2007, sets out the guiding principles and coordination arrangements for government and industry to develop joint strategies aimed at protecting the State's critical infrastructure.

The definition of critical infrastructure included in the CIP policy Framework was adapted from the national definition as follows:[34]

> *Critical infrastructure consists of those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of Victoria and its community.*

The CIP policy Framework is comprised of three main components:

- the identification and prioritisation of critical infrastructure;
- risk management; and
- roles, responsibilities and coordination arrangements.

Under the Framework, Victoria Police is the lead agency responsible for the identification and prioritisation of the State's critical infrastructure and also supports the Australian Security Intelligence Organisation (ASIO) in identifying national critical infrastructure located in Victoria. The Victorian critical infrastructure register is security classified and managed by Victoria Police.[35]

[34] Victorian Government, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007, p.6

[35] ibid., pp.8-9

The CIP policy Framework recommends that all owners/operators of critical infrastructure in Victoria adopt the same risk management procedures that owners/operators of declared essential services are required to comply with under the *Terrorism (Community Protection) Act 2003*.[36] Compliance with the policy framework by owners/operators however is not mandatory.

Also, the policy confers certain responsibilities on portfolio departments to ensure "adequate management" of security risks and emergencies within their relevant critical infrastructure sectors.

Under the CIP policy Framework, Victoria has adopted a sector based approach to the management of critical infrastructure consistent with the TISN national arrangements. The Framework lists nine industry sectors: Energy; Water; Transport; Communications; Health; Food Supply; Banking and Finance; Police and Emergency Services; and Places of Mass Gatherings (i.e. commercial centres, cultural, sport and tourism sectors). The policy notes that this last grouping is not strictly related to the definition of "critical infrastructure" but was included in the Framework as these areas were seen to be vulnerable to the same threats.[37]

The Committee notes recent advice from the DPC that, "places of mass gathering" are no longer recognised in the policy context as constituting critical infrastructure and risks associated with mass gatherings are now being coordinated at a national level by the NCTC and by Victoria Police at the state level.[38]

The Framework establishes Security and Continuity Networks (SCNs) in each of the industry sectors (similar to the Infrastructure Assurance Advisory Groups at the national level) to bring together government and critical infrastructure owners/operators to consider security, emergency management and business continuity policies and practices.[39]

2.5.3 Roles and responsibilities

The CIP policy Framework and Part 6 of the *Terrorism (Community Protection) Act 2003* assign specific roles and responsibilities to a number of public sector departments and agencies aimed at protecting the State's critical infrastructure from terrorism.

Department of Premier and Cabinet

Under the CIP policy Framework, the Security and Emergencies Unit (now known as the Security and Emergency Management Branch) within the DPC has the lead role for developing and coordinating whole-of-government CIP policy and strategy to ensure consistency across the government sector.

The Department's specific responsibilities under the CIP policy Framework include:[40]

[36] ibid., p.9

[37] ibid., p.7

[38] Department of Premier and Cabinet, *Review of the Arrangements for Managing Risk For Victorian Critical Infrastructure*, 15 June 2011, p.15

[39] Victorian Government, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007, pp.14-15

[40] ibid., p.17

- provide leadership and whole-of-government coordination in implementing Victoria's approach to critical infrastructure protection, including assisting the development of each SCN;
- work with regulating departments to develop relevant capabilities for critical infrastructure protection and ensure continuity of service;
- liaise with and support national CIP arrangements;
- communicate relevant intelligence and information to departments as required;
- participate in and support the national CIP arrangements for "mass gatherings"; and
- co-chair the Government Security and Continuity Network Coordination Group.

As noted the Premier is responsible for the administration of Part 6 of the Act. This makes the DPC responsible for ensuring that the provisions of the Act operate as was intended and for proposing amendments to the Act if required.[41]

Victoria Police

Under the CIP policy Framework, Victoria Police is the lead agency for the identification and prioritisation of the State's critical infrastructure. It also has specific responsibility to:[42]

- assist with the provision of protective security advice and develop counter-terrorism security strategies;
- gather and disseminate as required, relevant security intelligence;
- advise owners/operators of relevant threat information;
- provide protection for essential government services such as utilities and key facilities;
- liaise with owners/operators about the type of response expected for each type of threat/alert;
- conduct and participate in training exercises;
- participate in and support the national CIP arrangements; and
- co-chair the Government Security and Continuity Network-Coordination Group and the Police and Emergency Services SCN.

Victoria Police also has statutory obligations under Part 6 of the *Terrorism (Community Protection) Act 2003*. The Act prescribes that the Chief Commissioner must consult with the relevant Minister responsible for a declared essential service and the operator of the service

[41] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.6

[42] Victorian Government, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007, p.17-18

on the conduct of training exercises to test risk management plans and supervise the conduct of such training exercises.[43]

Other State government departments

A number of other State government departments have defined responsibilities under the State's CIP policy Framework in regards to: the management of security risks and emergencies relevant to their particular portfolio; the provision of strategic advice and coordination across the portfolio, including communication with the owners/operators of critical infrastructure; participation in the relevant industry SCN and provision of support to the national CIP arrangements. These agencies/departments are the:

- Department of Transport;
- Department of Sustainability and Environment;
- Department of Health;
- Department of Human Services;
- Department of Primary Industries;
- Department of Business and Innovation; and
- Office of the Emergency Services Commissioner (within the Department of Justice).

There have been some "machinery of government" changes since the release of the CIP policy Framework in April 2007 which have resulted in changes to the names of some of the departments listed in the policy document.

Under Section 27 of the *Terrorism (Community Protection) Act 2003*, the Premier may designate a "relevant Minister" in relation to a particular essential service. This results in the conferring of certain responsibilities under the Act with regard to determining the preparation of risk management plans by the operators of declared essential services and the testing of those plans through annual training exercises.

2.6 Recent developments

During the conduct of the audit and subsequent to the tabling of the Auditor-General's report in January 2009, a number of developments have taken place at both the national level and within the State in relation to national security, counter terrorism arrangements and the protection of critical infrastructure.

2.6.1 Recent developments at the national level

Significant developments have taken place in recent years at the national level in relation to national security issues, disaster management and critical infrastructure protection. Most of these have been agreed at COAG or through the NCTC and have the support of all Australian governments.

[43] *Terrorism (Community Protection) Act 2003*, s. 33

National Strategy for Disaster Resilience

On 7 December 2009, COAG agreed to adopt a whole-of-nation resilience based approach to disaster management which acknowledges that a national, coordinated and cooperative effort is required to enhance Australia's capacity to withstand and recover from emergencies and disasters. COAG also agreed to the establishment of a National Emergency Management Committee to drive and coordinate national policies and capability development in relation to emergency management.[44]

The National Emergency Management Committee subsequently developed the *National Strategy for Disaster Resilience*, adopted by COAG in February 2011. The purpose of the Strategy is to provide high-level guidance on disaster management to federal, state, territory and local governments, business and the non-profit sectors.[45] Some of the measures to be implemented by governments under the Strategy include:[46]

- jurisdictions should undertake disaster risk assessments for priority hazards over the next three years; and
- jurisdictions should maintain registers of significant risks to assist decision-making at all levels of government and by the private sector and communities.

While focussed on natural disasters, the Strategy notes that the approach outlined may also be applicable in preparing communities to deal with other disasters such as pandemic, animal disease outbreaks and terrorist incidents. The emphasis of the national strategy is on community resilience to disasters and other adverse events generally. The Strategy does not draw distinctions between "types" or causes of disasters but takes a holistic approach to disaster preparedness, response and recovery.

The Strategy states that governments are continually preparing for prevention, response and recovery activities and that there needs to be an acknowledgement that disaster resilience is a shared societal responsibility and not just the responsibility of emergency management agencies. In this way, disaster resilience seeks to build upon, rather than replace, existing strengths and arrangements.[47]

The *National Strategy for Disaster Resilience* is complemented by the following Commonwealth Government policy initiatives:

- *National Disaster Resilience Framework*;
- *Critical Infrastructure Resilience Strategy*;
- *National Climate Change Adaptation Action Plan*; and

[44] Australian Government, *Critical Infrastructure Resilience Strategy,* Commonwealth of Australia 2010, p.9

[45] Attorney-General's Department, Australian Government, *COAG adopts National Disaster Resilience Strategy,* February 2011, <http://www.ag.gov.au/www/agd/agd.nsf/Page/CouncilofAustralianGovernmentsMeeting>, accessed 9 June 2011

[46] Attorney-General for Australia, Media Release, *COAG adopts National Disaster Resilience Strategy,* 14 February 2011, <http://www.ema.gov.au/www/ministers/mcclelland.nsf/Page/MediaReleases-2011_FirstQuarter>, accessed 9 June 2011

[47] Australian Government, National Emergency Management Committee, *COAG National Disaster Resilience Statement, National Strategy for Disaster Resilience, Building our nation's resilience to disasters,* February 2011, p.3

- *National Partnership Agreement on Natural Disaster Resilience*.

Critical Infrastructure Resilience Strategy

In June 2010*,* the Australian Government released the *Critical Infrastructure Resilience Strategy*. This Strategy takes a more comprehensive approach to protecting the nation's critical infrastructure from "all hazards" (i.e. not strictly limited to the threat of a terrorist incident). The aim of the Strategy is to encourage critical infrastructure organisations, through a range of initiatives and activities, to better manage both foreseeable and unexpected risks to their assets, supply chains and networks.[48]

The Critical Infrastructure Resilience Strategy states:[49]

> *A resilience approach to managing the risks to critical infrastructure encourages organisations to develop more organic capacity to deal with rapid-onset shock. This is in preference to the more traditional approach of developing plans to deal with a finite set of scenarios.*
>
> *…The constantly changing nature (and accelerating rate of change) of the economy, technology and society mean that past events are not an adequate guide to determining plausible future hazards.*
>
> *…All decision makers, however, need to see all hazard risk mitigation and response as part of their role, and be empowered to carry it out….This gives organisations a greater ability to adapt to events that may have been unforseen or excluded from planning as being very low likelihood.*

The Strategy sets out the following six strategic imperatives aimed at building critical infrastructure resilience and achieving the Australian Government's aim:[50]

- operate an effective business-government partnership with critical infrastructure owners and operators;
- develop and promote an organisational resilience body of knowledge and a common understanding of organisational resilience;
- assist owners and operators of critical infrastructure to identify, analyse and manage cross-sectoral dependencies;
- provide timely and high quality policy advice on issues relating to critical infrastructure resilience;
- implement the Australian Government's Cyber Security Strategy to maintain a secure, resilient and trusted electronic operating environment, including for critical infrastructure owners and operators; and
- support the critical infrastructure resilience programs delivered by Australian states and territories, as agreed and as appropriate.

[48] Australian Government, *Critical Infrastructure Resilience Strategy*, 2010, p.4

[49] ibid., p.13

[50] ibid., p.4

A strong business-government partnership is the cornerstone of the Australian Government's approach to critical infrastructure resilience. As such, the TISN originally established in April 2003 as a forum for owners/operators of critical infrastructure and government representatives, continues to be an important component of the Australian Government's Strategy.

The "all hazards" approach to emergency management and the protection of critical infrastructure

As mentioned earlier, public policy is often developed in response to the most prominent community issues of the day and the development of specific terrorism focussed legislation and policy in Victoria in 2003 and 2007 was promulgated in response to the September 11 attacks in the United States and the terrorist incidents in Indonesia.

As noted, more recent incidents impacting Australia in the form of natural disasters have caused a policy shift at the Commonwealth level to building and promoting "disaster resilience" across the nation. In addition, the Australian Government has identified cyber security as a top national security priority and stresses the importance of cyber security to the protection of our critical infrastructure. This issue is gaining attention in response to the increasing complexity of operating systems and networks across a global environment and the accompanying rapid changes in technology.

Threats to critical infrastructure assets and the cessation or disruption of essential services are many and varied and becoming increasingly complex. Some of these threats can be foreseen and planned for and some may be completely unforseen. These threats obviously include the risk of a terrorist incident however, as indicated in recent policy developments at the national level, other risks and threats must also be considered and managed.

The Australian Government's *Critical Infrastructure Resilience Strategy* (2010) is directed at the continued operation of critical infrastructure *"*in the face of all hazards*"*.[51] Further the national TISN *"*operates on an all hazards basis*"*.[52]

At a state level, Victoria has had a long standing "all hazards" approach to emergency management. The "all hazards" approach to emergency management recognises that emergencies often require a similar response and that preparations for dealing with emergencies are fairly generic. This approach also recognises that one emergency can have a flow-on effect resulting in other emergencies.

The DPC has advised the Committee that the future strategic direction for the protection of the State's critical infrastructure will incorporate both resilience and an "all hazards" approach to risk management. This will be consistent with the emergency management approach already in place in Victoria and with the approach outlined in recent national policy.[53]

[51] ibid., p.25

[52] ibid., p.16

[53] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.3

2.6.2 Other recent reviews impacting emergency response and the management of critical infrastructure in the State

2009 Victorian Bushfires Royal Commission

The 2009 Victorian Bushfires Royal Commission found that five of the 15 fires which started on Black Saturday were as a result of the failure of electricity assets/infrastructure. The Commission recommended urgent preventative steps be taken to address the State's ageing electricity infrastructure. The Commission's report states that fire starts involving electricity assets have been "*one of the primary causes of catastrophic fires in Victoria during the past 40 years*."[54]

Ironically, the fire in Kilmore East, which was purportedly caused by failures in electricity infrastructure, threatened the Kilmore Water Treatment Plant (designated critical infrastructure managed by Goulburn Valley Water). In fact, the control building at the treatment plant, containing chemical dosing equipment and control equipment, was completely destroyed. Power supplies to the Broadford Water Treatment Plant and Clonbinane areas were also affected.[55]

The Royal Commission was of the view that Energy Safe Victoria should take a more proactive role as the electricity industry safety regulator in monitoring the compliance of energy owners/operators stating:[56]

> *In the past it has taken a largely passive role, focussing on confirming distribution businesses' bushfire mitigation plans and line clearance plans. It has not assessed in detail whether safety objectives contained in the Electricity Safety Act 1998 are actually being achieved…*
>
> *Overall the Commission is strongly of the view that Energy Safe Victoria's regulatory powers and resources need to be strengthened, including the organisation's ability to apply sanctions for non-performance.*

2010-11 Victorian floods response

Between September 2010 and February 2011, the State experienced widespread flood damage across a number of Victorian communities. In fact, the floods in January 2011 in central and western Victoria placed the Kerang high-voltage terminal station under threat. Extensive sand bagging and channelling was required during the emergency to protect against a major shutdown of power to around 20,000 households in the north-western areas of Victoria.

In February 2011, the Premier instigated a review of Victoria's flood warnings and response efforts. An Interim Report was released in July 2011.

The Interim Report presents a summary of the work undertaken to date as part of the review process and identifies a number of major issues and key themes emanating from the review work. Findings and recommendations are to be included in the Final Report, due in

[54] 2009 Victorian Bushfires Royal Commission, *Final Report — Summary*, July 2010, p.12

[55] B. Anderson, Goulburn Valley Water, *Lessons from the 'Black Saturday' Fires,* paper presented at 72nd Annual Water Industry Engineers and Operators' Conference, Bendigo, September 2009, pp.105-6

[56] 2009 Victorian Bushfires Royal Commission, *Final Report — Summary*, July 2010, pp.12-13

December 2011. It is anticipated that the Review will examine relevant legislation, policy, procedures, systems and structures to assess whether the arrangements meet community expectations and provide the State with an appropriate framework to manage large scale emergencies.[57]

While the Interim Report does not include firm conclusions and recommendations as such, the head of the review team, Mr Neil Comrie, does make the following observations about emergency management arrangements in Victoria:[58]

> *…the Review team is of the strong view that …the current legislation, policy and structures that constitute the emergency management framework in Victoria is of major concern. This framework does not effectively support an "all hazards" approach to emergency management.*
>
> *Based on my experience as the Bushfires Royal Commission Implementation Monitor and on the evidence already to hand at the Review, I have concluded that there are fundamental flaws in the Victorian emergency management framework.*
>
> *Although the clear intent of the Emergency Management Act, the State Emergency Response Plan and the Emergency Management Manual Victoria is to provide for an 'all hazards", "all agencies" approach to emergency management, this has not occurred in reality. In the absence of an effective enabling policy framework to "drive" this philosophy, the emergency services agencies in Victoria operate in a siloed structure with each agency focussed on legislated obligations to address specific hazards.*
>
> *…Immediate action is required to reconstruct the relevant legislation, policy, procedures and structures to deliver an effective "all hazards", "all agencies" approach to emergency management in Victoria.*

Green Paper: Reform of Victoria's emergency management arrangements

Following on from the Government's response to the recommendations made by the Victorian Bushfires Royal Commission and the Victorian Floods Review Interim Report, on 12 September 2011, the Victorian Government released a Green Paper for discussion on Victoria's crisis and emergency management arrangements: *Towards a More Disaster Resilient and Safer Victoria*.

The Green Paper states that the findings of both the 2009 Victorian Bushfires Royal Commission and the Victorian Floods Review indicate that the existing crisis and emergency management legislation, policy, governance and operational arrangements in the State require an overhaul to meet future challenges.[59]

[57] Victorian Government, Victorian Floods Review, *Review of the 2010-11 Flood Warnings and Response – Interim Report*, 30 June 2011, p.13

[58] ibid., p.26

[59] Victorian Government, Department of Premier and Cabinet, Security and Emergency Management Branch, *Towards a More Disaster Resilient and Safer Victoria, Green Paper: Options and Issues*, September 2011, p.1

The Green Paper identifies a range of issues and options relating to Victoria's capacity for planning, preparedness, prevention, response and recovery from large-scale emergencies. The Paper focuses on two key concepts:[60]

- emergency service organisations and government agencies working with communities to plan and prepare for disasters; and
- realising an "all hazards, all agencies" approach to managing large scale disasters.

The Paper lists 32 options for consideration across the following areas:[61]

- oversight and coordination of the system;
- capacity and capability;
- service delivery performance; and
- building community resilience.

It is noted that the Government aims to build resilience across the community by assisting households, private sector businesses and community groups to be informed, fully and actively engaged in emergency preparedness and better equipped to respond in the event of an emergency. The Government was seeking public comment and feedback on the Green Paper until 14 November 2011. It is intended that following the receipt of the Final Report on the *Review of the 2010-11 Flood Warnings and Response* in December 2011, the reform proposals will be released in a White Paper during the first half of 2012.[62]

In the interim, the Government states that it intends to continue its implementation of the recommendations from the 2009 Victorian Bushfires Royal Commission and any immediate responses required to the Final Report of the Victorian Floods Review.[63]

[60] Victorian Government, Department of Premier and Cabinet, Security and Emergency Management Branch, *Victoria Prepared: An Action Plan*, September 2011

[61] ibid.

[62] ibid.

[63] ibid.

CHAPTER 3: FINDINGS AND RECOMMENDATIONS OF THE AUDITOR-GENERAL

3.1 Introduction

In January 2009, the Auditor-General released his report entitled *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*. The objectives and scope of the audit were outlined in Chapter One of this report. The main findings were contained in two chapters covering governance and compliance. As noted earlier, the chapter on "Funding" did not contain any significant issues or recommendations.

The report made a number of recommendations which were in the main directed at the Department of Premier and Cabinet (DPC) and to a lesser extent Victoria Police. There were also two minor recommendations directed at the "lead" departments with responsibility for overseeing the owners/operators of critical infrastructure within industry groups relevant to their particular portfolios.

The following paragraphs present a summary of the recommendations made, details of the initial responses from the departments/agencies and an update of actions taken subsequently to address the issues raised and implement the Auditor-General's recommendations.

3.2 Terrorism: prevention and preparedness

The nature of a terrorist attack makes it extremely difficult to prevent. Prevention efforts rely mainly on security intelligence and physical security measures. Efforts to minimise the impact of a terrorist act require individuals, organisations and countries to be as best prepared as possible in terms of planned response and recovery.

Preparedness is essentially about good planning and requires:

- detailed planning (incorporating risk management and crisis management);
- clearly defined and commonly understood roles and responsibilities (governance structures/frameworks);
- regular testing and training of crisis management plans and emergency response plans (through simulations and training exercises); and
- adequate funding/resources.

These elements were the focus of the Auditor-General's review.

3.3 Auditor-General's recommendations

The Auditor-General made eleven recommendations in his report. Seven recommendations were directed at addressing issues related to governance arrangements and four recommendations were related to matters of compliance.

Overall, the audit found that the governance arrangements in place to protect the State's essential services and critical infrastructure could be more effective and made a number of recommendations directed at addressing deficiencies in that area. The Auditor-General expressed the view that, whilst the responsibility for the oversight of operators of essential services in specific sectors rests with the relevant "lead" department, the DPC needed to exercise firmer leadership in administering the provisions of Part 6 of the *Terrorism (Community Protection) Act 2003* (the Act) and in the implementation of the Critical Infrastructure Protection Framework.[64]

In relation to matters of governance, the Auditor-General recommended that the DPC:[65]

- establish clear oversight and coordination of the arrangements for both Part 6 of the *Terrorism (Community Protection) Act 2003* and the CIP policy 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 policy 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 the CIP policy 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); and

- 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).

One governance related recommendation was directed to all of the "lead departments" audited to obtain the necessary security clearances so that appropriate officers could access information relevant to their sectors (Recommendation 4.7).[66]

With respect to compliance issues, the Auditor-General made the following four recommendations directed at the DPC and Victoria Police together.[67]

- 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

[64] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.6

[65] ibid.

[66] ibid., p.7

[67] ibid.

implementing Part 6 of the Act and the CIP policy 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 policy Framework to promote greater consistency and to enable better identification of lessons learned and continuous improvement (Recommendation 5.3); and
- 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).

3.4 Agency responses

The response by the DPC included in the Auditor-General's report was generally supportive of the findings and indicated that a review of the critical infrastructure arrangements were underway and that the review's terms of reference included consideration of the findings and recommendations made in the audit report.[68]

The Department did not agree, however, with the Auditor-General's view that the DPC should take a more proactive oversight role in relation to the implementation of the legislation and accompanying policy and procedural arrangements. The Department responded in the Auditor-General's report that while Part 6 of the Act is administered by the Premier, the legislation also provides that the Premier designate responsible ministers who are then each accountable for certain activities under the Act.[69] The DPC provided a lengthy response to the report which was included as Appendix C in the Auditor-General's report.

While noting the comments and findings made in the Auditor-General's report, the responses from Victoria Police and other audited departments were generally supportive of the current CIP arrangements.

In December 2009, the *Response by the Minister for Finance to the Auditor-General's Reports issued during 2008-09* (Minister for Finance Report) was tabled. This report provides an opportunity for portfolio departments to inform the Parliament and the public on issues and actions taken in respect to the Auditor-General's recommendations. In this report responses were provided from each of the portfolio departments which had been included in the audit *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*.

In the Minister for Finance Report, the DPC indicated that it supported two of the eleven recommendations (i.e. Recommendations 4.6 and 4.7) and "supported in part/ principle" the remaining nine, stating that they would be addressed as part of the review

[68] ibid., p.11

[69] ibid., p.79

of the CIP arrangements. The response also stated that the Review had commenced and recommendations from the Review were anticipated to be complete in the first part of 2010.[70]

3.5 The Department of Premier and Cabinet Review of critical infrastructure arrangements

As part of the Committee's follow-up, the Committee noted the release in 2009 of a Discussion Paper prepared by the DPC entitled, *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure.*

The Committee wrote to the Department in May 2011 requesting advice on the status of the Review of the CIP arrangements and the progress made on implementation of the Auditor-General's recommendations.

The Department advised the Committee that in late 2008, the previous Government had agreed to review the CIP arrangements. Stimulus for the review came from:[71]

- increased stakeholder interest in the policy area;
- the need for arrangements to remain relevant and comprehensive; and
- the Auditor-General's performance audit.

The Department's Discussion Paper described the current arrangements and posed a number of questions for reflection and consultation with stakeholders. Submissions were requested by 30 October 2009. The DPC advised that a literature review had also been undertaken as part of the review process to investigate international best practice.[72]

Seventeen submissions were received from stakeholders and the DPC engaged a consultant to meet with 120 individual stakeholders through a series of group sessions.[73]

The DPC advised that a final report containing recommendations had been submitted to the Government for consideration and was expected to be finalised in the middle of the year. The Department advised that the delay in finalising the review has been caused by a number of natural disasters occurring in Victoria during 2009-10. Also, the Department was mindful that any changes should take account of developments at the national level and therefore some delay was due to the completion of national reviews which were underway.[74]

Given that two and a half years had passed since the Auditor-General's report was tabled, the Committee was keen to assess the extent to which the Auditor-General's recommendations had been addressed through the DPC Review. As such, the Committee requested a copy of the Department's final report (DPC Review Report) on the review. This was provided to the Committee on 19 July 2011.

[70] Department of Treasury and Finance, *Response by the Minister for Finance to the Auditor-General's Reports issued during 2008-09,* December 2009, p.103

[71] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.2

[72] ibid., p.3

[73] ibid.

[74] ibid., p.5

The DPC Review Report contains five recommendations aimed at improving the effectiveness of Victoria's arrangements for managing risks to essential services and critical infrastructure including consideration of the recommendations made in the Auditor-General's January 2009 audit report.

At the public hearing, the Secretary DPC, commented that the Department had devoted significant attention to the 2009 Review undertaking wide consultation and a literature review. The Review also included serious consideration of the recommendations made by the Auditor-General.[75]

The Secretary stated that actions had already been taken to address immediate concerns in relation to the identification of critical infrastructure; improving collaboration between government-industry; providing early warning to industry of potential hazards; and reporting on exercises and other activities to key government forums.[76]

Subsequent to the public hearing, the Committee sought further information about the status of the DPC Review Report. The DPC advised that copies of the Report had been made available to relevant government and industry stakeholders in the critical infrastructure and essential services sphere.[77]

In relation to formal adoption of the DPC Review Report by the Government and plans for a revision of the policy framework, the DPC advised the Committee that:[78]

> *The Government noted the review, but did not formally endorse it. However, the CGRC* [Central Government Response Committee] *has previously endorsed the review recommendations which are largely administrative in nature or proposed additional work. It should be noted that the review recommendations included the development of a new framework under the Act.*
>
> ...
>
> *Under section 38 of the Terrorism (Community Protection) Act 2003, amended this year, a review of the whole Act is to be completed by 30 June 2013. As part of this review it is open to the Government to further consider the operation of Part 6.*

The Department also advised that a revised policy Framework would be developed during 2012 and was anticipated for release in early to mid 2013.[79]

The findings and recommendations contained in the DPC Review Report have been reviewed by the Committee as part of its Inquiry.

[75] Ms H. Silver, Secretary, Department of Premier and Cabinet, transcript of evidence, Session 2, 25 August 2011,p.4

[76] ibid.

[77] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 20 October 2011, p.1

[78] ibid., p.19

[79] ibid.

3.6 Other recent developments

As noted in Chapter Two of this report, during the conduct of the Auditor-General's audit and subsequent to the tabling of his report in January 2009, a number of changes have taken place at the national level in relation to the focus of national security, counter terrorism arrangements and protection of critical infrastructure which has had a flow on effect to Australian state and territory jurisdictions. These developments need to be taken into account as part of this Committee's inquiry.

In relation to these developments, the DPC advised in its correspondence to the Committee in June 2011:[80]

> *There has been a significant paradigm shift in the management of risk to essential services and critical infrastructure since the Auditor-General's audit.*
>
> ...
>
> *Victorian agencies propose to incorporate resilience and an all hazards approach in policy development, as opposed to focussing on protection of specific critical infrastructure against terrorism. This approach recognises that the key risks to critical infrastructure are from natural hazards rather than terrorism related, but that governments and owners and operators must be prepared to respond and recover from all threats.*

Given the impending changes to policy in this area, the following chapters of this report focus on those areas considered to be the key and persistent issues raised in the Auditor-General's report, namely issues surrounding:

- governance (roles, responsibilities and accountability);
- risk management (planning preparedness and review); and
- compliance of owners/operators of critical infrastructure and essential services with legislation and policy.

The Committee considers that these are the key areas which need clarification and simplification in the development of any new policy or amendments to the legislative framework.

3.7 Future focus – Findings of the Committee's Inquiry

The challenge in CIP management for government in the future is to address the issues identified and lessons learned from the last few years' operation of Part 6 of the *Terrorism (Community Protection) Act 2003* and the *Victorian Framework for Critical Infrastructure Protection from Terrorism* (CIP policy Framework). In addition, developments in national policy and changes in the risk environment have highlighted new issues which must be taken into consideration in order that requirements remain meaningful and relevant.

[80] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.3

The Auditor-General's findings have largely been verified by the findings of the DPC's own review of CIP risk management arrangements and the Committee understands that some changes have been made, and others are intended, to address weaknesses and limitations identified.

What remains as a point of contention is the role of the DPC in these management arrangements. This matter is discussed in detail in Chapter Four of this report.

The current CIP policy Framework forms the management model for critical infrastructure protection in the State. The question is how can that model be improved? Based on a review of the material and evidence presented to the Committee by the DPC, Department of Justice (i.e. Victoria Police), and Auditor-General, and a review of the relevant literature, the Committee has concluded that there are a number of key issues which must be addressed to improve public sector administration of CIP arrangements. These are as follows:

- the need for the provision of clear and strong central policy leadership and coordination within a "devolved" system of administration and implementation;
- clearly and commonly understood terminology and definitions and roles and responsibilities of all stakeholders;
- a formalised and commonly understood process for the identification and classification of critical infrastructure (including essential services);
- standardised application of CIP requirements across categories of "criticality";
- the consideration of all risks and hazards, and in particular other "high/catastrophic impact", "low probability" risks and hazards;
- a formal and standardised system of compliance certification and reporting; and
- incorporation of the Council of Australian Governments (COAG) agreements on a uniform approach to disaster management resilience and critical infrastructure protection.

The opportunity to address these issues presents now in the redrafting of the *Victorian Framework for Critical Infrastructure Protection from Terrorism* policy document and also in the forthcoming review of the *Terrorism (Community Protection) Act 2003*, due for completion in June 2013.

It is hoped that the recommendations put forward by the Committee in this follow-up inquiry to the Auditor-General's report will also assist in improving the management of critical infrastructure protection arrangements by the Victorian public sector.

CHAPTER 4: GOVERNANCE AND ACCOUNTABILITY

4.1 Introduction

Governance is generally understood to encompass authority, stewardship, leadership, direction and control. Governance refers to the way an organisation is managed and held to account in the achievement of its strategic and operational objectives.

Effective governance arrangements ensure that responsibilities and accountabilities are clearly understood and objectives and outcomes can be achieved while complying with the relevant legal and policy obligations.

In the case of the State's critical infrastructure assets and services, the governance arrangements should also provide a solid and well coordinated mechanism for the protection of the infrastructure from all potential risks and threats, including acts of terrorism. Good governance also includes systems for monitoring performance to assist in the achievement of objectives and outcomes.

While governments have a role to play in the protection of critical infrastructure, it is a matter of responsibility and good corporate governance that owners/operators of critical infrastructure address the security of their assets and ensure that processes have been established to protect business continuity. The *Victorian Framework for Critical Infrastructure Protection from Terrorism* (CIP policy Framework) and Part 6 of the *Terrorism (Community Protection) Act 2003* (the Act) outline the roles and responsibilities of government agencies and owners/operators (private and public) of critical infrastructure and essential services in managing the threat of a terrorist incident.

4.2 Components of the governance arrangements surrounding the State's critical infrastructure

4.2.1 Legislation and policy

The Critical Infrastructure Protection (CIP) legislation and policy together establish the governance arrangements for managing the protection of the State's critical infrastructure. The *Terrorism (Community) Protection Act 2003* establishes mandatory risk management obligations for owners/operators of declared essential services and the CIP policy Framework provides non-mandatory guidelines for owners/operators of critical infrastructure; outlines the roles/responsibilities of relevant government agencies; and establishes the Security and Continuity Network (SCN) structure to facilitate dialogue between government and industry groups.

One of the main purposes of the *Terrorism (Community Protection) Act 2003* was to provide new powers and obligations relating to the prevention of, and the response to, terrorist acts and also to provide for the operators of certain essential services to prepare risk management plans.[81] Under Part 6 of the Act, a "relevant Minister" can direct an operator to comply with the provisions of the Act and where this is unsuccessful seek an order form the Supreme Court of Victoria to enforce compliance.

[81] *Terrorism (Community Protection) Act 2003*, s. 1

The CIP policy Framework recommends "*that all owners/operators of identified critical infrastructure adopt the risk management procedures that declared essential services are required to follow*".[82] The practices outlined in the Framework are voluntary. There are no penalties for non-compliance.

Hence, the major distinctions between the legislation and the policy are that the legislation is mandatory and relates to "essential services infrastructure" while the policy is non-mandatory and relates to "critical infrastructure".

4.2.2 Committees and networks

As stated, in Victoria the ownership of critical infrastructure is vested in a mix of public and private entities with a significant proportion of essential services owned and/or operated by private sector corporations. As such, the State government has recognised that building effective relationships and partnerships between government agencies and industry owners/operators is fundamental to achieving the optimum outcome in ensuring the State is best prepared to respond to the impact of an emergency incident on essential services and critical infrastructure.

The SCN Structure forms "*the heart of the Victorian CIP management arrangements.*"[83] Under the Framework it was intended that a SCN would be created in each of nine industry sectors with the objective of bringing together state and local government agencies with the owners/operators of critical infrastructure to consider matters concerning security, emergency management and business continuity. This structure mirrors the national CIP government-industry partnership approach and enables linkages between state and national industry-based groups.[84]

Each sector is linked to a lead department which chairs and administers the network to facilitate industry-government partnerships to consider and manage the relevant issues surrounding security, emergency management and business continuity policies and practices.[85]

The CIP policy Framework also established the Government Security and Continuity Network-Coordination Group (SCN-CG) comprising the Chairs of each of the SCNs and a representative from Victoria Police's Critical Infrastructure Protection Unit (CIPU) and the DPC's Security and Emergency Management Branch. The SCN-CG is "co-chaired" by Victoria Police and DPC with the Security and Emergency Management Branch providing secretariat support.

Sitting over the SCN structure is the Central Government Response Committee (CGRC) which is chaired by the Secretary, DPC and comprises deputy secretary level representatives from each department, a Deputy Commissioner of Victoria Police and the Emergency Services Commissioner.[86] The CGRC is a specific interdepartmental standing committee responsible for coordinating whole-of-government response to extreme emergency incidents

[82] Victorian Government, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007, p.9

[83] ibid., p.14

[84] ibid.

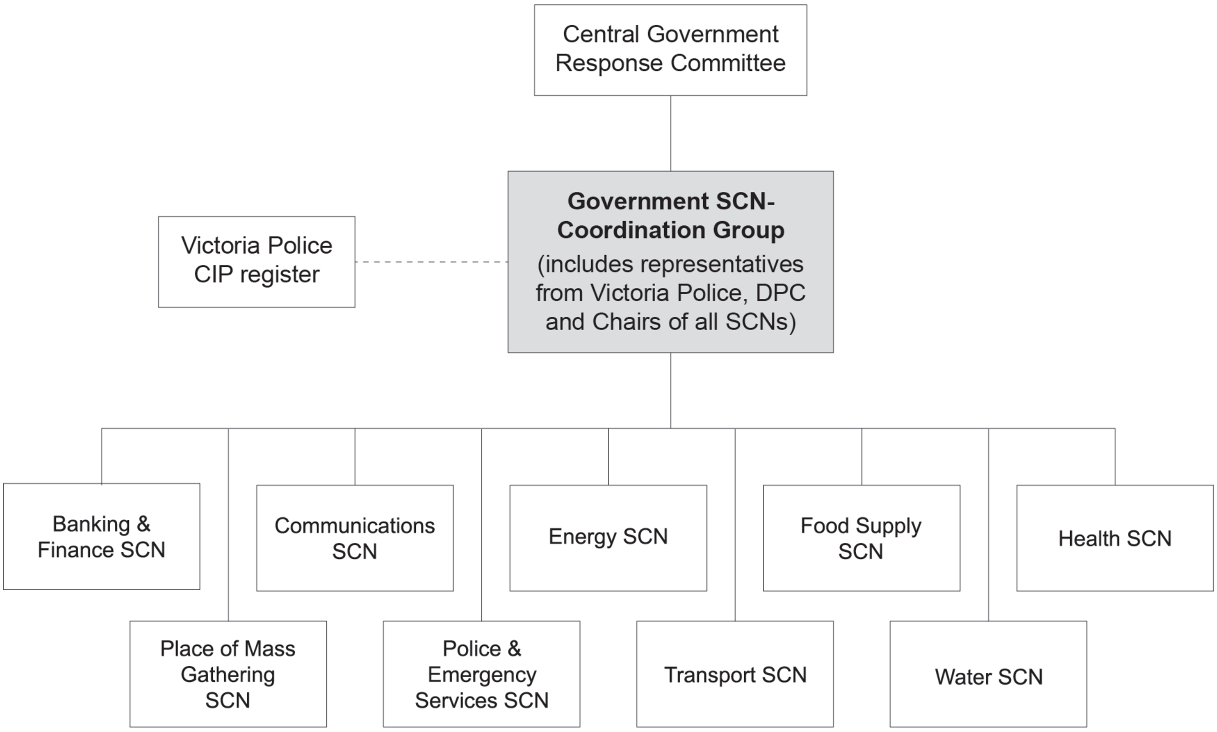
[85] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, pp.28-9

[86] ibid., p.26

in Victoria and for providing advice to the Security and Emergencies Committee of Cabinet (SECC).

The following diagram taken from the CIP policy Framework shows the cascading system of committees and networks which comprise the CIP management structure in Victoria.

Figure 4.1: Victorian CIP management structure


Central Government Response Committee
Victoria Police CIP register
Government SCN-Coordination Group (includes representatives from Victoria Police, DPC and Chairs of all SCNs)
Banking & Finance SCN
Communications SCN
Energy SCN
Food Supply SCN
Health SCN
Place of Mass Gathering SCN
Police & Emergency Services SCN
Transport SCN
Water SCN

Source: Victorian Government, 'Victorian Framework for Critical Infrastructure Protection from Terrorism', April 2007, p.15

The Committee considers that the CIP management structure as depicted in Figure 4.1 is deficient and should be revised to provide a more comprehensive and accurate representation of the CIP governance structure in the State including arrangements under Part 6 of the Act and clearly showing the DPC as the accountable and responsible agency, and representing the Premier as the "Minister" with ultimate responsibility for overseeing critical infrastructure protection arrangements across the whole-of-government.

4.3 Auditor-General's findings

The Auditor-General's report included a chapter dedicated to reviewing the effectiveness of the governance arrangements in place to protect the State's critical infrastructure and essential services. In particular, the Auditor-General assessed:

- the adequacy of oversight and coordination by the DPC;
- whether roles and responsibilities of Victoria Police and other "lead" departments/ agencies had been clearly defined and were being performed effectively;
- whether adequate systems were in place for monitoring implementation of the legislative and policy requirements;
- the identification and effective management of inter-agency risks;

- the effectiveness of the Security and Continuity Network; and
- whether mechanisms were in place to assist effective communication and consultation between relevant parties.

In relation to the State's CIP governance arrangements, the Auditor-General concluded that:[87]

> *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 policy Framework and remove barriers to their effective implementation.*

Further findings in relation to CIP governance arrangements were as follows:[88]

- the co-existence of Part 6 of the Act covering essential services risk management and the policy Framework for critical infrastructure protection, is somewhat confusing to agencies and inhibits coordination;
- SCNs are not all fully operational, with varying levels of progress. Two of the nine were found to be operating well. Three had not been established at all and timeframes for implementation of the SCN structure had not been determined;
- the effectiveness of the SCN-CG had been impacted by delays in the implementation of the SCN structure and the co-chairing arrangements between the DPC and Victoria Police. The Auditor-General found that the DPC had taken the dominant role and considered that more equal input from DPC and Victoria Police would provide opportunities for improved coordination between the administration of the Act and the requirements for Victoria Police under the CIP policy Framework.[89] The focus of the SCN-CG on critical infrastructure and not also declared essential services has limited its effectiveness as an oversight committee;
- the roles and responsibilities of agencies in relation to critical infrastructure protection are unclear;
- efforts to clearly identify and mitigate inter-agency risks associated with whole-of-government arrangements for managing the protection of the State's critical infrastructure were limited; and
- an adequate performance monitoring framework was not in place for assessing the effectiveness of the State's arrangements for the protection of critical infrastructure and essential services from terrorism.

The Auditor-General made seven recommendations in relation to addressing these shortcomings in governance arrangements. Actions taken by the DPC and Victoria Police to address the recommendations since the tabling of the Auditor-General's report together with other subsequent developments have been reviewed by the Committee and are discussed in the following sections.

[87] ibid., p.6

[88] ibid., p.40

[89] ibid., p.27

4.4 Audit recommendations and actions taken to date

4.4.1 Oversight and coordination of critical infrastructure protection arrangements

The Auditor-General recommended that the DPC establish clear oversight and coordination arrangements for both Part 6 of the *Terrorism (Community Protection) Act 2003* and the CIP policy Framework by an appropriate body such as the SCN-CG (Recommendation 4.1).[90]

Response by the Department of Premier and Cabinet

As already noted, the DPC provided a lengthy response to the Auditor-General which was included as Appendix C to the report. In this response the DPC made the following points:[91]

- Part 6 of the legislation is administered by the Premier who (together with the DPC) is responsible for ensuring that the provisions of the Part operate as intended and remain relevant;
- Part 6 of the legislation provides for the Premier to designate responsibilities to relevant ministers who must ensure compliance with the provisions of the legislation; and
- DPC will consider the "intent" of the Auditor-General's recommendation as part of a review of the critical infrastructure arrangements noting that it *"would be against best practice for DPC to take an operational role in the management of these activities."*

Subsequent developments noted by the Committee

The Committee notes that the issue of what constitutes appropriate oversight by the DPC and the role of the DPC in the State's CIP arrangements was the main point of contention between the Auditor-General and the Department.

In responding to the DPC's response, regarding its role in this area, as included in the audit report, the Auditor-General stresses that he does not advocate an operational role for the DPC but that some central oversight and monitoring is required by the Department to ensure that the provisions of the Act are operating as intended and to identify and assist in overcoming any difficulties in interpretation and application of the Act.[92]

As part of its Inquiry, the Committee wrote to the Department and the Auditor-General seeking further comment in relation to their differing views in an effort to clarify the issue and resolve the disagreement.

[90] ibid., p.41

[91] ibid., pp.79-80

[92] ibid., p.12

Auditor-General's view of the Department of Premier and Cabinet's role in critical infrastructure protection

In correspondence provided to the Committee in April 2011, the Auditor-General advised that the DPC's response to the audit regarding its central agency role in the area of critical infrastructure protection and particularly in relation to the operation of Part 6 of the Act *"goes to the heart of the issue of what is appropriate oversight; particularly where responsibility for policy and implementation are separate."*[93]

In further correspondence to the Committee in June 2011 regarding this issue, the Auditor-General makes the point that a number of audits have raised similar issues in terms of oversight roles which has led the Auditor-General to conclude:[94]

> *It is clear from these audits that there is a systemic issue relating to what can be termed an "oversight deficit" by agencies which has resulted in a blurring of accountability.*

In relation to the recommendation in his report, the Auditor-General advised the Committee that the DPC needed to exercise firmer leadership in administering Part 6 of the Act and implementation of the CIP policy Framework to assist in their effective implementation.[95] In particular he states there is a need for the DPC to:[96]

- clarify the roles and responsibilities of owners/operators and portfolio departments/ agencies; and
- provide guidance to assist owners/operators of critical infrastructure satisfy their obligations under Part 6 of the Act.

Department of Premier and Cabinet's view of its role in critical infrastructure protection arrangements

The Committee wrote to the DPC in May 2011 requesting further explanation regarding this point of contention with the Auditor-General over the role of the Department in oversight and coordination of the CIP arrangements.

In June 2011, the DPC advised the Committee that in terms of its responsibilities for oversight of Part 6 of the Act, the "relevant Ministers" (as designated by the Premier) are responsible for ensuring that the provisions of the Act are complied with (i.e. that risk management plans have been prepared and audited and that declared essential service operators undertake training exercises to test those plans at least once each year). The DPC states:[97]

[93] Mr D. Pearson, Victorian Auditor-General, *Review of VAGO audit reports tabled January to June 2009,* letter to the Committee, received 19 April 2011, p.1

[94] Mr D. Pearson, Victorian Auditor-General, *Inquiry into Auditor-General's Report No.15: 2008-09, Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure,* correspondence to the Committee, received 1 June 2011, p.2

[95] ibid.

[96] ibid., p.5

[97] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.6

> *As the Auditor-General was advised, the DPC wrote to Victorian Ministers to advise them of their responsibilities as 'relevant Ministers' under the Act. This role does not make DPC responsible for the implementation of the Act at an operational level.*

The Department added that central oversight of the Act is provided through its co-chairing of the SCN-CG which allows each of the SCN chairs to share information on best practice and ensure compliance with provisions of the Act.[98]

The Department made the following additional points in relation to this issue:[99]

- misunderstanding of DPC's role has led to a perception that the Department is responsible for implementation activities that are the responsibility of other entities;
- the findings of the DPC's review of the arrangements for critical infrastructure risk management, has confirmed that the Department's role should be one of strategic leadership, rather than coordination or governance;
- coordination and governance roles rest with Victoria Police as is consistent with current practice; and
- this approach is also supported by nationwide research conducted by the DPC where operational responsibility for preparedness to respond to terrorism incidents relating to critical infrastructure and essential services is carried out by police. This is considered "best practice".

Evidence taken at the public hearing

In response to questions raised at the hearing concerning the DPC's role, the Secretary of the Department stated:[100]

> *The DPC's role we see as strategic – that is, to provide policy leadership in this area and to advise in relation to legislative arrangements. We also have an important role in ensuring that in processes that are set up there are adequate systems that monitor those processes and, where appropriate, we are engaged in that monitoring and evaluation, and there will be different levels of that.*

The Secretary, DPC advised the Committee that the monitoring of critical infrastructure arrangements occurs through the Department's policy oversight role, its joint chairing with Victoria Police of the SCN-CG and through the oversight of the SCN arrangements via the CGRC, chaired by the Secretary, DPC.[101]

In terms of monitoring compliance with Part 6 of the Act, the Department stressed to the Committee that in a devolved model of shared responsibility, it is clearly the responsibility of the relevant Minister and department to lead implementation and monitor compliance with the

[98] ibid.

[99] ibid., p.7

[100] Ms H. Silver, Secretary, Department of Premier and Cabinet, transcript of evidence, Session 2, 25 August 2011, p.6

[101] ibid.

legislation. The role of the DPC relates to ensuring there are strong reporting arrangements in place through the SCN-CG and the CGRC to obtain assurance that there is legislative compliance.[102]

The Secretary acknowledged that the gaps identified by the Auditor-General in his report together with the review of arrangements undertaken by the Department had indicated that action was needed, and is now being taken, to strengthen the monitoring framework in terms of the reporting which occurs to the SCN-CG and also that Group's reporting to the CGRC. The DPC has also identified a need to strengthen and assist the development of some of the "less mature" SCNs.[103]

In summing up at the conclusion of the hearing with representatives from the DPC and Victoria Police, the Auditor-General remarked:[104]

> *…there is something missing still, because we are talking about committees and co-chairs and all this sort of thing, and that just does not fit the bill in terms of accountability. Committees are great for consultation, for co-ordinating views and for things like that …but I am left with a question mark about: Where does the executive responsibility and leadership lie and who is executing that role?*

Committee review and discussion

Given the extent of the fundamental disagreement between the Auditor-General and the DPC regarding the role of the Department in the oversight of CIP arrangements and subsequent comments made by the Auditor-General to the Committee in both past reports and recent discussions concerning "the appropriate role for a central agency in monitoring and overseeing policy implementation", the Committee took the opportunity of exploring this issue in some further detail.

The role of the central agency

In a letter to the Committee in October 2010, the Auditor-General in commenting on the reports which had been issued by his Office between July and December 2008, stated:[105]

> *Unfortunately, many of the persistent governance weaknesses you identify continue to appear in more recent audits.*
>
> *For example, our 2009-10 audits have increasing shown the need for greater clarity around the roles of Departments and central agencies in monitoring, guidance and compliance, challenging the effectiveness of "arm's length" accountability approaches often adopted in the Victorian public sector.*

[102] Ms H. Silver, Secretary, and Mr D. Speagle, Deputy Secretary, Federalism, Citizenship and Climate Change, Department of Premier and Cabinet transcript of evidence, Session 2, 25 August 2011, pp.8-9

[103] Ms H. Silver, Secretary, Department of Premier and Cabinet, transcript of evidence, Session 2, 25 August 2011, p.7

[104] Mr D. Pearson, Victorian Auditor-General, Victorian Auditor-General's Office, transcript of evidence, Session 4, 25 August 2011, p.11

[105] Mr D. Pearson, Victorian Auditor-General, letter to the Committee, received 6 October 2010

The key questions emanating from the Auditor-General's review of CIP governance arrangements are:

- What level of accountability does the central agency have in a situation where they administer legislation and policy but the implementation is devolved to other public sector agencies?

- Is it the Premier who is ultimately accountable through his Department for ensuring that the State is well prepared to respond to threats to its critical infrastructure and essential services?

Traditionally speaking, central agencies play a central role in policy formulation and coordination across the whole-of-government. In Victoria, these agencies are the DPC and the Department of Treasury and Finance (DTF). Notably, with some exceptions, central agencies seldom carry direct responsibility for a particular set of policies but rather take the job of influencing and coordinating the policy initiatives in line departments through policies which set the direction and priorities of the Government. The activities of central agencies are critical to effective government particularly where policies apply across government departments (as in the case of social policy) or across sectors (as in the case of critical infrastructure protection).

Central agencies may also see their role as including an educatory role for other public sector agencies and an advisory role for the Premier/Treasurer and other Ministers. The World Bank notes, central agencies are the "buckles" which link the political and administrative parts of the public sector "*and as such are crucial elements in any process of governance*".[106] It goes on to posit that there are five fundamental activities for central agencies:

- advising;

- appointing;

- coordinating;

- monitoring; and

- regulating.

For each of these activities, the role of linking the political to the administrative in government is important. Central agencies must simultaneously "manage up" to ministers and "manage down" to department/agencies and their executives. Increasingly central agencies have had to also "manage out" by relating the work of government to private sector organisations and other non-government organisations.

The role of central agencies in western democracies has been impacted by numerous reforms in public administration over recent years. Many administrative reforms have had decentralisation as one of their goals but in many cases the overall effect has been to centralise control in these central agencies. This is partly because coordination becomes even more crucial when so much else in the public sector becomes decentralised, devolved,

[106] The World Bank, 'Center of Government', 8 February 2001, <web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTPUBLICSECTORANDGOVERNANCE/EXTADMINISTRATIVEANDCIVILSERVICEREFORM/0,,contentMDK:20133433~menuPK:1919171~pagePK:210058~piPK:210062~theSitePK:286367,00.html>, accessed 30 June 2011

privatised and outsourced and partly because of the need to drive reforms within a particular department and/or across government agencies.

As the DPC has been keen to point out, in our Westminster system of government, Ministerial accountability to the Parliament is a fundamental element in assessing the diligent and effective management of assets and resources and the achievement of strategic policy outcomes. Individual agencies/departments and their senior executives also play a significant role in implementing the appropriate operational initiatives and reforms, policies, processes and functions to achieve broad government objectives and requirements. This takes the form of internal accountability between the agencies/departments and their Ministers. The issue then becomes, what systems or mechanisms are in place to provide the Government and Parliament with some surety or confidence that departments are in fact implementing the policy as intended?

Where a policy applies to the management of resources or the delivery of services (such as, critical infrastructure assets and the provision of essential services) by a party outside the public sector, the line of accountability is more devolved and even more complex.

A recent Australian National University discussion paper on public sector accountability notes:[107]

> *…the whole issue of how far governments are accountable for outsourced services has been the subject of continuing disagreement. On the one hand, advocates of outsourcing have steadfastly maintained that governments remain as accountable for outsourced services as they are for services provided in house (Industry Commission, 1995). Outsourcing, it has been argued, may devolve responsibility but not accountability.*

So, in terms of public accountability, the demands are essentially the same whether the services are provided publicly or privately. This then presents governments with a new element of added risk, given that they cannot exercise the same degree of control over contractors or private sector providers as they can over their own departmental officers. To reduce this risk, governments place contractual obligations on private providers, establish grievance procedures, such as through an ombudsman, and create legislative requirements or regulations which must be met.

And so, in the case in point, the Victorian Government has been mindful that a large proportion of the State's critical infrastructure and essential services are managed by private sector organisations. Given the importance of this infrastructure to the economic and social well-being of the Victorian public, the Government has sought to influence the management and oversight of these entities through legislation and policy. Mandated legislative requirements have been attached to those assets determined to be the most "essential" to the well-being of the Victorian community and to focus risk management on the risk considered to have the highest impact but also which may be considered as "low" in terms of likelihood of occurrence (i.e. the risk of a terrorist incident).

At the crux of the disagreement between the Auditor-General and the DPC seems to be the difference in opinion about whether:

[107] R. Mulgan, Asia Pacific School of Economics and Government, Australian National University, *Accountability in a Contemporary Public Sector,* November 2005, p.12

- Monitoring and oversight constitutes an operational role or responsibility?
- A government committee constitutes effective central oversight and accountability?

Regarding this different view, the Assistant Auditor-General, Performance Audit made the following observation at the hearing:[108]

> *…there is a misapprehension of what we are saying and* [the DPC's] *interpretation of what we are saying. They say, quite properly, that the secretaries of the departments and the responsible ministers under each area have responsibility and accountability, and we did not dispute that. They go on to say that therefore they should not have an operational role, and we do not dispute that. What we are arguing is that you need this monitoring and oversight role. If they want to characterise that as an operational role, we would debate that it is an operational role. We actually see it as a strategic role. I do not think we have ever been able to get agreement there to then have an argument about what follows from that.*

The "strategic" role of the Department of Premier and Cabinet

Also relevant to this area of discussion is the role of the Department as stated in its Annual Report and on its website. The Department's *2010-11 Annual Report* states that:[109]

> *DPC supports the government in four key ways:*
>
> – *Supporting the Premier, as head of Government and Cabinet, and Minister for the Arts*
>
> – *Providing strategic policy leadership and directions across Victoria's public service*
>
> – *Developing and coordinating whole-of-government initiatives*
>
> – *Delivering whole-of-government services and programs relating to government information, communication and the arts.*

In the area of critical infrastructure protection, the DPC has advised the Committee that they see their role as "strategic". So what does a "strategic role" encompass? Generally speaking, literature describes strategic management as: specifying goals and objectives; developing policies and plans to achieve those objectives; and evaluating performance to assess the achievement of those objectives. Strategic management provides overall direction and involves an ongoing process of evaluation to reaffirm direction and make adjustments if necessary.

As such, from the view of a central agency such as the DPC, devolved from operational implementation of the provisions of Part 6 of the Act and the guidelines established in the CIP policy Framework, being strategic should be about the Department's ability to "see the big picture" or the overview. However, it is the Committee's view that the DPC appears to

[108] Mr A. Greaves, Assistant Auditor-General, Performance Audit, Victorian Auditor-General's Office, transcript of evidence, Session 1, 25 August 2011, p.5

[109] Department of Premier and Cabinet, *2010-11 Annual Report,* 2011, p.1

have given limited attention to what needs to be identified, measured and reported in order to obtain a picture of what is actually transpiring and to provide information on which to make decisions about either, the need for legislative amendment, or further guidance to stakeholders, or changes to the policy, to ensure that implementation is effective in achieving the desired outcomes.

The Committee notes the DPC's *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure* (DPC Review Report) to Government which contains a section on "Leadership and Governance" and which states in the opening paragraph:[110]

> *The need for defined, stronger leadership and clearer governance guidelines and structures was emphasised in the review.*

In this section of the Report the DPC persists with its view that the recommendation of the Auditor-General that the DPC establish clear oversight and coordination for Part 6 of the Act is an operational role. The Report states it is the Department's view that its "*strategic leadership function would be compromised if it were responsible for 'operational aspects' of the Framework."*[111]

Further in relation to leadership by the SCN-CG (co-chaired by the DPC), the Report states that *"the SCN-CG could be more robust in providing leadership and direction"* and recommends that the CGRC collectively, and its members individually, take an active oversighting role of the work of the SCN-CG which *"may provide greater accountability, clearer direction for the sectors and a higher level of authority for departmental members to act."*[112]

In relation to the issue of "governance", the DPC Review Report discusses issues surrounding interpretation of the legislation, whether there is a need for the legislation to be more prescriptive, and the oversight of declared essential service operators by government departments. At no point is the DPC noted as having a governance role to play in relation to the provisions of the Act but rather states:[113]

> *While recognising the usual roles, authority and responsibilities of government departments, Victoria Police agree that they are well placed to lead implementation, monitoring and coordination of the arrangements.*

The Report goes on to recommend that Victoria Police lead a working group of government department and industry representatives to develop guidance in relation to the requirements of Part 6 of the Act.[114]

Finally in the conclusion to its Report, the DPC makes it clear that it does not accept responsibility for any overall governance of the arrangements and clearly wishes to devolve any responsibilities to other government departments. The DPC Review Report states:[115]

[110] Department of Premier and Cabinet, *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure*, 15 June 2011, p.11

[111] ibid., pp.11-12

[112] ibid., p.12

[113] ibid., p.14

[114] ibid.

[115] ibid., p.16

> *Further work to articulate the requirements of the arrangements, whether legislative or policy; better understanding by all stakeholders of the aims and objectives of the arrangements through a revised Framework; and a good governance structure* ***led by the appropriate government departments*** *will all serve to enhance the partnership and contribute towards security and social and economic well-being for all Victorians.* (emphasis added)

Committee findings and recommendations

The Committee acknowledges that privatisation and corporatisation of the State's critical infrastructure means that the Victorian government is removed from direct control over the management and protection of those critical infrastructure assets and services. The onus is on the owners/operators of critical infrastructure to ensure that they undertake adequate risk management of their assets and ensure that they comply with all relevant legislation and licensing regulations regarding safety and training exercises etc. The Committee also notes, however, that in reality there is an expectation on the part of the Victorian community that the Government will ensure the continuation of essential goods and services and in the event of a disruption to those services (such as in the case of the Longford gas explosion) it is government which is immediately called to answer for, and respond to, the disruption.

The Committee has reviewed the material provided by the DPC and heard evidence from representatives of both the DPC and Victoria Police about the governance and oversight arrangements in place for critical infrastructure protection in terms of joint government-industry committees and central coordination committees.

Based on this evidence, the Committee has concluded, in concord with the Auditor-General, that the governance and accountability arrangements, as have been operating, are seriously lacking in terms of the adequacy of central monitoring and oversight of the application of Part 6 of the Act and the CIP policy Framework across public sector agencies.

The Committee found that the DPC has a very different philosophy of what an appropriate governance structure constitutes and the role of the Department in that structure. The Department has indicated that it considers that governance and accountability best sits within a committee structure made up of a collective group of players of which one is the DPC. The extent of their role as a "player" in these arrangements appears to be limited to certain "co-chairing" responsibilities as is the case with the SCN-CG and in "chairing" by the DPC Secretary of the CGRC. For the rest, the Committee found that the DPC views Victoria Police and individual relevant departments as the accountable entities in the State's CIP arrangements both legislative and policy.

These representations by the Department have led the Committee to conclude that since Part 6 of the Act came into effect in 2004 and the CIP policy Framework in 2007, the DPC has not accepted and continues to dispute its obligations and responsibilities in co-ordinating the effective application and implementation of the arrangements. Further, it is the view of the Committee that the Department have been remiss in adequately supporting the Premier, as the head of Government, in executing his responsibilities for administering Part 6 of the Act and as the central agency responsible for the whole-of-government application of the CIP policy Framework. The Committee considers this to be unacceptable. This ongoing failure potentially leaves the Premier, as head of government, exposed to high level public criticism for any failure in the protection of essential services and critical infrastructure, particularly considering that the matter has now been subject to an Auditor-General's report and with the tabling of this report.

In support of these conclusions, the Committee notes the following points which are clearly at odds with the DPC's continuing position that it does not have ultimate responsibility for central governance of the arrangements in place to protect the State's critical infrastructure and essential services:

- the Premier is the responsible "Minister" for the administration of Part 6 of the Act supported by his department, the DPC, for ensuring the provisions operate as intended and amendments to the legislation are proposed where necessary;[116]

- the CIP policy Framework issued by the DPC in 2007 clearly states *"the DPC has the lead role in developing and coordinating whole-of-government strategy and policy for CIP to ensure a consistent approach across government*";[117] and

- the DPC has undertaken a significant review of the arrangements stretching over three years in duration and has now issued its Report to Government on its findings and recommendations relating to both the application of Part 6 of the legislation and the principles provided in the CIP policy Framework.

These points indicate that the Department has not been adequately performing its own stated role in ensuring the provisions of Part 6 of the Act are operating as intended and effectively co-ordinating the CIP policy arrangements as a whole-of-government strategy.

The Committee notes the comments made by the Secretary, DPC, at the hearing that the Department has acknowledged that the monitoring arrangements undertaken by the SCN-CG and the CGRC require strengthening and that efforts have been instigated to achieve this. Also that the SCN structure needs further development to ensure it is operating effectively. While the Committee looks forward to these enhancements to the monitoring and reporting activities of these committees it does not consider that these committees provide the level of accountability demanded by both the best principles of public sector governance and the seriousness of the management issues involved.

As stated, the Committee is concerned that there remains a persistent reluctance on the part of the Department in accepting the ultimate accountability for CIP arrangements in the State of Victoria in line with its role as the agency primarily responsible for administration of Part 6 of the Act and the agency responsible for the development of critical infrastructure policy in the State. It is the finding of this Committee, without reservation, that responsibility for the effective application of the legislation and policy cannot be completely devolved to either Victoria Police or to individual departments. The DPC must be accountable and must desist from continuing to avoid its obligations and responsibilities in this area by taking a much stronger role in monitoring performance, providing guidance and encouraging compliance across the Victorian public sector and amongst industry stakeholders and in adequately supporting the Premier, as head of Government and as the "Minister" responsible for CIP arrangements in the State.

[116] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.6

[117] Victorian Government, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007, p.17

Recommendation 2:

The Committee recommends that, as a matter of good governance and due and proper accountability and assurance, the Department of Premier and Cabinet take a greater lead in providing guidance and monitoring compliance as part of their strategic responsibilities for the oversight of critical infrastructure protection arrangements in Victoria. Such strategic oversight and monitoring should include:

(a) An appropriate system of internal accountability between itself and departments/agencies implementing the *Victorian Framework for Critical Infrastructure Protection from Terrorism* policy and the provisions of Part 6 of the *Terrorism (Community Protection) Act 2003*;

(b) The identification of the key critical infrastructure protection policy outcomes and performance measures against which the effectiveness of departments' and agencies' critical infrastructure protection arrangements can be assessed; and

(c) A comprehensive reporting system to enable monitoring of outcomes and the status of implementation across departments/ agencies to identify factors impacting upon the desired outcomes and areas for improvement.

Recommendation 3:

The Committee recommends that the critical infrastructure protection management structure as depicted in the Department of Premier and Cabinet's policy documentation be revised. Such revision should clearly show the Department of Premier and Cabinet as the agency ultimately responsible for overseeing management arrangements across the whole-of-government for the protection of both critical infrastructure and declared essential services and their responsibility to the Premier as the "Minister" accountable to the Parliament for these arrangements.

4.4.2 Development of a performance management framework

The Auditor-General recommended that the Department of Premier and Cabinet lead the development of a performance management framework for monitoring and reporting on the implementation of both Part 6 of the Act and the CIP policy Framework. Further, the performance management framework should include key indicators, targets and reporting arrangements for assessing the extent to which departments, agencies and industry have fulfilled their obligations in addition to measures for monitoring the achievement of joint objectives (Recommendation 4.2).[118]

Response by the Department of Premier and Cabinet

The response provided by the Department in the *Response by the Minister for Finance to the Auditor-General's Reports 2008-09 (*Minister for Finance Report) in December 2009 stated that Victoria had *"developed devolved arrangements that make owners and operators (of*

[118] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.41

critical infrastructure) and relevant Ministers and departments responsible for monitoring compliance with the Act and framework in accordance with best practice."[119]

Further the DPC stated that the intent of this recommendation would be considered as part of the review of CIP arrangements underway.[120]

Subsequent developments noted by the Committee

The Committee wrote to the DPC in May 2011 requesting further information in regard to the action taken to address the Auditor-General's recommendations. The Department provided the Committee with a copy of the Discussion Paper issued in 2009, *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure* (DPC Discussion Paper). Other material provided to the Committee by the DPC indicated that the Department considered the recommendation relating to the development of a performance management framework should be led by Victoria Police.[121]

The DPC Review Report to Government indicates that the DPC views this recommendation as an operational responsibility rather than a strategic one.[122] The Report goes on to recommend that Victoria Police lead a working group of government department and industry representatives to develop guidance notes to establish a common understanding of the requirements of Part 6 of the Act.[123]

Evidence taken at the public hearing

At the public hearing, representatives from the Department were questioned further on the issues surrounding monitoring and reporting. The Secretary of the DPC stated that the Department managed its oversight responsibilities in three ways:[124]

- by monitoring the framework under which the risk to critical infrastructure is managed;
- through its chairing of the CGRC which receives *"regular reports from the Security and Continuity Networks on progress and key issues";* and
- through its co-chairing with Victoria Police of the SCN-CG which includes the chairs of each of the eight SCNs.

In elaborating further, the Secretary, DPC advised that the SCN-CG receives the minutes of the other SCNs and can check progress on the work being undertaken by those network groups. Also the Committee was advised that the reporting from the SCNs to the CGRC had been strengthened. Progress reports were made by the SCN-CG to the CGRC in 2008 and 2010. Also any matters associated with security and terrorism related issues are reported to

[119] Department of Treasury and Finance, *Response by the Minister for Finance to the Auditor-General's Reports issued during 2008-09*, December 2009, p.103

[120] ibid.

[121] Ms H. Silver, Secretary, Department of Premier and Cabinet, *Attachment C, Victorian Auditor-General's Recommendations Cross Reference*, letter to the Committee, received 17 June 2011

[122] Department of Premier and Cabinet, *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure*, 15 June 2011, pp.11-12

[123] ibid., p.14

[124] Ms H. Silver, Secretary, Department of Premier and Cabinet, transcript of evidence, Session 2, 25 August 2011, p.6

the CGRC and the Security and Emergencies Committee of Cabinet. The Secretary of DPC advised that as chair of the CGRC, she had been briefed in the past on key projects and achievements surrounding critical infrastructure arrangements in the State.[125]

At the hearing with representatives from the Department of Justice and Victoria Police, the then Acting Chief Commissioner of Police provided the Committee with some detail as to the work of the CIPU within Victoria Police. The Unit maintains records of critical infrastructure site visits and subsequent reports to the owners/operators and regional emergency management members. It also stores records of training exercises in relation to declared essential services conducted under the provisions of Part 6 of the Act. The Committee was advised that owners/operators are not under any obligation to comply with recommendations made by Victoria Police in relation to their terrorism risk management plans however they are encouraged to consider any recommendations and work with the relevant government department in order to achieve appropriate outcomes.[126]

In terms of the reporting arrangements in relation to training exercises conducted under the Act, Victoria Police advised that it makes a report on the outcomes of the exercises to the relevant Minister and the department responsible for that industry group also makes a report. This is in addition to the report made by the local area command to the operator. The Committee was advised that when they are testing the adequacy of the exercises, there must be specific objectives and outcomes in place against which the exercise can be tested.[127]

The Committee was advised that in addition to the responsibilities conferred on Victoria Police under the Act, arrangements have been developed within Victoria Police requiring the local police commander to make at least two contacts each year with critical infrastructure operators within their local area to update emergency contact lists and report on those.[128]

Further information sought from the Department of Premier and Cabinet

Subsequent to the hearing the Committee requested further details from the DPC in relation to the monitoring activities and “measures” used by the Department to assess the effectiveness of the management arrangements in place to protect the State’s essential services and critical infrastructure. The DPC advised that in addition to its chairing and secretariat duties, DPC staff regularly:[129]

- participate in SCN meetings and exercises as appropriate;
- review SCN meeting minutes;
- follow-up on issues raised by SCNs as part of their SCN-CG secretariat responsibilities; and

[125] ibid., p.7

[126] Mr K. Lay, Acting Chief Commissioner of Police, Victoria Police, transcript of evidence, Session 3, 25 August 2011, p.3

[127] Mr S. Fontana, Assistant Commissioner of Police, State Emergencies and Securities Department, Victoria Police, transcript of evidence, Session 3, 25 August 2011, p.6

[128] ibid.

[129] Ms H. Silver, Secretary, Department of Premier and Cabinet, *Issues requiring further clarification*, letter to the Committee, received 20 October 2011, p.7

- liaise with portfolio departments in monitoring developments in the critical infrastructure risk management sphere.

In addition, the DPC advised that regular interaction with officers in responsible departments enables a view to be compiled as to the adequacy of the program and regular interaction with Victoria Police (who oversight exercises under the Act) also provides insight.[130]

In addition to these "measures", DPC also seeks information from departments, to provide to the CGRC, on the progress of arrangements for managing risk for critical infrastructure and essential services within their portfolio sectors. Reports are due in October 2011 and as noted at the hearing previous reports were provided in 2008 and 2010.[131]

The Committee requested copies of the "progress reports" made to the CGRC in 2008 and 2010 and found that:

- the June 2008 "progress report" comprised an agenda item from the SCN-CG to the CGRC advising that a SCN All Sectors Forum was scheduled for late October 2008 and proposing "*that the SCN-Coordination Group formally report biannually to the CGRC and additionally as required on planning and preparedness by Victorian critical infrastructure sectors who provide essential services";*[132] and
- the October 2010 "progress report" to the CGRC comprised a background brief for the Chair in regard to the SCN-CG report which requested that the CGRC agree to annual reporting by the SCN-CG on planning and preparedness by critical infrastructure sectors who provide essential services and note the second SCN All Sectors Forum in March 2010; the establishment of SCNs in the Communications, and Banking and Finance sectors; and the completion of the final draft report of the Review of CIP arrangements.[133]

In relation to the performance of the DPC itself in effectively oversighting critical infrastructure arrangements in the State, the Committee requested information from the Department on the development of specific performance indicators, targets, key measures or regular reports it used to assess its performance.

The Department advised that the devolved nature of the arrangements, "*in which DPC's role is strategic oversight, makes it difficult for DPC to quantify or measure its own performance.*"[134]

In performing its strategic oversight role, the DPC advised that it considers the following factors important:[135]

- reporting and communication networks should be transparent, effective and accessible;

[130] ibid., p.9

[131] ibid., p.7

[132] Ms H. Silver, Secretary, Department of Premier and Cabinet, *Issues requiring further clarification*, *Central Government Response Committee, 25 June 2008, Agenda Item 6*, letter to the Committee, received 20 October 2011

[133] ibid. *Agenda Item 3*, letter to the Committee, received 20 October 2011

[134] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 20 October 2011, p.15

[135] ibid.

- Departments should understand and perform their responsibilities under Part 6 of the Act;
- Departments should understand and perform their responsibilities under the CIP policy Framework; and
- there should be appropriate identification of issues to senior officers, committees or Government.

The DPC also advised the Committee that it assesses its performance in relation to these factors through discussions with staff from other government departments in forums such as the SCN-CG and participation in the SCNs and through its reports to the CGRC. Further assessment is made in terms of the nature of the reports received and the issues discussed by senior committees and with government stakeholders. The DPC considers that involvement and response to recent events such as the Morwell land slip, the February floods and the September 2011 avian paramyxovirus outbreak *"are indicators that the reporting chains and networks are working well."* The DPC states that it also assesses the success of initiatives in which it participates through forums such as the SCN-CG and the CGRC however it notes these are not quantified outside of its annual reporting to the CGRC.[136]

The Department acknowledges that there is always room for improvement and that the DPC strives to achieve continuous improvement and evolution in its performance management arrangements.[137]

Further information sought from the Department of Justice

The Committee also wrote to the Department of Justice (DOJ) requesting details of their response to the view of the DPC advising that Victoria Police is the lead agency responsible for implementation of the audit recommendation to develop a performance management framework for measuring, monitoring and reporting on the implementation of Part 6 of the Act and the CIP policy Framework.

The DOJ advised the Committee that the recommendation made in the DPC Review Report was for Victoria Police to take the lead on developing guidance notes for critical infrastructure operators relating to measuring, monitoring and reporting on the implementation of Part 6 of the Act. The Department advised that the CIPU of Victoria Police will commence the project soon. The Department stressed that the project will produce "guidance notes" only and that uptake by owners/operators will be voluntary with no authority for police of government departments to enforce any particular aspects of the notes.[138]

The performance of a training exercise conducted by operators of a declared essential service under Part 6 of the Act is supervised by police and the relevant government department. The DOJ advised the Committee that there is no set structure for this monitoring, however Victoria Police use an accepted evaluation form throughout the exercise to determine whether the operator has satisfied requirements. Police then provide a formal report to the operator and discuss any findings. A letter is forwarded to the Minister of the relevant government departments advising of the conduct and adequacy of the exercise. There is no associated

[136] ibid.

[137] ibid.

[138] Ms P. Armytage, Secretary, Department of Justice, letter to the Committee, received 13 October 2011, pp.3-4

reference in the Framework for critical infrastructure operators unless they are also a declared essential service. The DOJ advised that Victoria Police officers with responsibility for emergency management in the regions and local police officers maintain contact with critical infrastructure owners/operators in their areas and undertake training exercises and familiarisation of their sites.[139]

Committee findings and recommendations

The Committee found very little evidence that any serious consideration has been afforded the Auditor-General's recommendation relating to the development of a performance management framework to assess the implementation and effective operation of the CIP policy Framework. In terms of Part 6 of the Act, there is more formal documentation and recording in place by Victoria Police and in those departments overseeing the more well established industry sectors such as water, energy and transport to ensure compliance with the risk management provisions of the legislation. However, the Committee was unable to assess the extent or quality of higher level performance management information including the development of key performance measures/indicators for assessing how well departments are managing their obligations in relation to critical infrastructure protection.

Evidence given at the hearing by representatives of the DPC in relation to performance reporting and measurement was abstract and lacking in structure and detail. References were made to "briefings on key projects and achievements", "progress reports in 2008 and 2010" and "mechanisms through the CGRC" for providing assurance.[140]

The Committee also found that any discussion of performance monitoring in regard to the implementation of either the CIP policy Framework or Part 6 of the Act is virtually non-existent in the DPC Review Report and there are no recommendations made in the Review Report which address the Auditor-General's recommendation for the development of a performance management framework.

Further correspondence provided by the DPC in October 2011 indicates that the Department considers it difficult to quantify or measure its own performance in terms of its strategic oversight of the CIP arrangements. In addition, the attention on performance monitoring by Victoria Police is firmly focussed on its statutory obligations in regard to supervising exercises conducted by the operators of declared essential services under Part 6 of the Act, with no indication of their undertaking any broader performance assessment activities.

The Committee notes also that the Auditor-General's report stated that departmental performance monitoring systems for assessing progress and successful implementation of the requirements of Part 6 of the Act and the CIP policy Framework were limited and many were in need of development.[141] The Committee has not sought any evidence through this Inquiry to enable it to make a current assessment of the extent and quality of performance evaluation undertaken by relevant departments overseeing the management of critical infrastructure by operators within their portfolios. However, the Committee considers these departmental

[139] ibid., pp.4, 6

[140] Ms H. Silver, Secretary, Department of Premier and Cabinet, transcript of evidence, Session 2, 25 August 2011, pp.7-8

[141] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.39

systems to be an important component of a comprehensive performance evaluation system for the management and protection of critical infrastructure and essential services in the State.

Further, the Committee considers strategic management to be an important element in effective public sector governance. As noted in the previous section of this report, the implementation of strategic government policy requires a system of internal accountability between the agencies implementing the actions outlined in the policy and the agency responsible for strategic oversight of that policy which in this case is clearly the DPC.

An essential component of this system of internal accountability and effective policy implementation is a methodology or framework which enables implementation of the policy to be monitored to assess the extent to which policy objectives are being successfully achieved and to highlight any "problem" areas and allow for review and improvement. For example, misunderstanding or misinterpretation of the terminology used in the policy, disagreement about the need for certain actions to be taken and/or lack of expertise or resources to implement the policy.

In reinforcing the Auditor-General's recommendation, the Committee found that greater attention needs to be given to developing a more formalised structure of performance evaluation in relation to monitoring, measuring and reporting on how well:

- operators/owners of critical infrastructure and essential services are fulfilling their CIP obligations;
- relevant departments/agencies (including Victoria Police) are performing their legislative and policy responsibilities; and
- the DPC is performing its strategic leadership and oversight role.

The DPC, Victoria Police and relevant departments need to give consideration to identifying the key information or activities which identify performance in the area of CIP and develop a system of reporting which enables a comprehensive and meaningful assessment of CIP in the State. Further, the DPC and Victoria Police could identify examples of "best practice" in relevant departments from which other departments can seek to improve their performance in the area of CIP management. This issue is discussed in further detail in the following section.

Recommendation 4:

The Committee recommends that the Department of Premier and Cabinet re-consider the Auditor-General's recommendation relating to the development of a performance measurement framework for critical infrastructure protection arrangements in Victoria. Consideration should be given to the development of relevant indicators which assess the extent to which the policy framework is being implemented across departments/agencies and highlighting any areas which may require investigation or attention.

Recommendation 5:

The Committee recommends that the Department of Premier and Cabinet consider and identify key information and indicators to evaluate how well the Department is performing in terms of its own strategic leadership and oversight of critical infrastructure (including essential services) protection arrangements in the State of Victoria.

Recommendation 6:

The Committee recommends that all government departments with responsibilities in relation to declared essential services under Part 6 of the *Terrorism (Community Protection) Act 2003* and with responsibilities for the protection of critical infrastructure in the State have appropriate systems in place to monitor and report on their own management performance, to assist proper accountability and identify and drive improvement where needed.

Recommendation 7:

The Committee recommends that Victoria Police develop a more formalised internal management reporting system which enables an assessment to be made of their performance in relation to their training exercise supervisory responsibilities under Part 6 of the *Terrorism (Community Protection) Act 2003* and also in relation to their responsibilities under the *Victorian Framework for Critical Infrastructure Protection from Terrorism*, and any subsequent iteration of the policy.

4.4.3 Clarification of roles and responsibilities

The Auditor-General recommended that the DPC clarify the roles and responsibilities of departments and agencies under Part 6 of the Act and CIP policy Framework in an effort to reduce confusion and gaps (Recommendation 4.3).[142]

Response by the Department of Premier and Cabinet

The response provided by the Department in the Minister for Finance Report stated that the roles and responsibilities of relevant parties were being considered in the review of the CIP arrangements underway. Also that Victoria had instigated a review by the Commonwealth of the national arrangements to clarify roles, responsibilities and definitions in the area.[143]

Subsequent developments noted by the Committee

The Committee wrote to the DPC in May 2011 seeking an update on the status of the Commonwealth's review of the national terrorism security arrangements and how this had reduced confusion within Victorian government departments and agencies over roles, responsibilities and definitions.

The Department advised that significant changes in the management of critical infrastructure protection have taken place both nationally and internationally. Whilst Australia had originally adopted most of the terminology and analyses from the United States immediately following the September 11 events, it has been recently recognised that this terminology does not necessarily best reflect the current Australian context.[144]

[142] ibid., p.41

[143] Department of Treasury and Finance, *Response by the Minister for Finance to the Auditor-General's Reports issued during 2008-09*, December 2009, p.104

[144] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.7

A number of reviews in relation to the protection of critical infrastructure and terrorism security have been undertaken by the Commonwealth and also in a number of other states. The DPC advised that all these reviews have addressed similar issues, namely:[145]

- the role of government in relation to privately owned infrastructure;
- differences between protecting critical infrastructure from the threat of terrorism as opposed to "all hazards" generally; and
- defining what constitutes critical infrastructure.

In terms of the action taken by the DPC to clarify definitions and responsibilities following these reviews, the Department advised that the national review had been endorsed by COAG in December 2009 and had been considered as part of the Victorian review of CIP arrangements to ensure alignment between the State and the Commonwealth. The Department advised that key themes from the *National Strategy for Disaster Resilience* will be incorporated into a revised policy framework for Victoria.[146]

The DPC advised that the consultation undertaken with 120 individual stakeholders as part of the Department's review of CIP arrangements had found little confusion on the functions of the Victorian government and agencies and the Commonwealth government. However, it was noted that clearer delineation was sought between the roles of the DPC and Victoria Police.

In relation to its own role, the DPC advised the Committee that:[147]

> *The review of the arrangements for managing risk to Victorian critical infrastructure has confirmed that DPC's role should be that of strategic leadership, rather than coordination or governance. Victoria Police agree that they are responsible for coordination and governance, in accordance with the review findings and current practice.*

The DPC advised the Committee that it has been agreed that DPC has a strategic leadership role while Victoria Police is responsible for the operational activities such as implementation and coordination.

The DPC Review Report recommends that clarification of the roles and responsibilities of departments and agencies under the CIP policy Framework and the legislation be addressed in two ways as follows:[148]

- a working group of government departments and industry representatives, led by Victoria Police, will be established to develop guidance notes to ensure a common understanding of the requirements of Part 6 of the *Terrorism (Community Protection) Act 2003*; and

[145] ibid., p.8

[146] ibid.

[147] ibid., p.7

[148] Department of Premier and Cabinet, *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure*, 15 June 2011, p.14

- leadership under the Framework will be clearly defined to identify and reflect the roles of the DPC and Victoria Police and the roles and responsibilities of individual Ministers and government departments.

Committee findings and recommendation

Victorian government departments and agencies have specific roles to play in relation to:

- executing their obligations under Part 6 of the Act in relation to declared essential services within their department's purview; and
- performing their role and responsibilities as set out in the CIP policy Framework as they relate to the protection of critical infrastructure within their department's purview.

Following on from the findings of the Auditor-General, the Committee notes that the DPC Review Report has acknowledged that:

- a lack of definition and prescription in the Act in relation to the audit of risk management plans and the assessment of exercises to test those plans has led to individual interpretations by Victoria Police and government departments;[149]
- government departments have a varied range of roles and responsibilities in the Framework. The understanding of these roles and responsibilities is diverse and has resulted in inconsistent and variable resourcing, participation and sector leadership;[150] and
- limited guidance available to government departments has led to inconsistency and inability to benchmark for best practice, particularly in relation to exercising and auditing under Part 6 of the Act.[151]

In addressing these deficiencies the DPC Review Report states that the Framework will be revised to more clearly define its objectives and accurately describe the roles and responsibilities of government departments and industry users, and also government departments will be consulted to develop an agreed view about their roles and responsibilities in the new Framework.[152]

The Committee looks forward to greater clarification and more definitive description of the roles and responsibilities of government departments and agencies under a revised CIP policy Framework as foreshadowed by the DPC in its Review Report. Further, the recommendation in the DPC Review Report to form a working group to provide guidance and develop a common understanding of the requirements under Part 6 of the Act is considered to be a positive move in this direction. However, the Committee is concerned to ensure that any clarification of roles and responsibilities makes it clear, as concluded earlier in this report, that the DPC is the agency with ultimate responsibility for the oversight and governance of critical infrastructure and essential services protection in the State.

[149] ibid., p.6

[150] ibid., p.13

[151] ibid.

[152] Department of Premier and Cabinet, *Report to Government, Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure*, 15 June 2011, pp.9, 13

As noted in the previous section of this report (refer 4.4.2), the Committee considers that it may be a useful exercise for the DPC and Victoria Police to identify and highlight "best practice models" within government departments which could provide guidance for the development of procedures and systems in other less well developed departments in the management of declared essential services and critical infrastructure.

The Committee notes that the Auditor-Generals' report made the following observations in relation to those departments with good management practices in place:

- in relation to communication within the SCN structure, the Auditor-General noted that the Department of Transport (DOT) was *"the better practice agency in raising issues/ updating the CGRC on critical infrastructure protection issues for the two sectors it manages"*;[153]

- the Department of Primary Industries (DPI) (Energy sector), the Department of Sustainability and Environment (DSE) and the DOT had all provided oversight and assistance to operators of declared essential services to assess and prioritise risks and develop risk management plans;[154]

- DSE provides oversight for operators in the water sector in relation risk assessment advice and guidance for asset management based on an "all hazards, all agencies" approach. Information identified from assessments was forwarded by the DSE to Victoria Police for consideration to assist in the identification of critical infrastructure in the sector;[155]

- DPI (Energy sector), DSE and DOT were all actively engaged with work being undertaken by the Commonwealth in relation to the development of Critical Infrastructure Protection Modelling and Analysis (CIPMA) to examine relationships and interdependencies between critical infrastructure systems;[156] and

- the DSE had developed appropriate processes to facilitate compliance with Part 6 of the Act.[157]

Based on the observations made in the Auditor-General's report, it is evident that there are a number of best practice models for the management and oversight of the protection of the State's essential services and critical infrastructure within the Victorian public sector which could be adapted and applied across other government departments with similar responsibilities.

[153] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.36

[154] ibid., p.49

[155] ibid., p.50

[156] ibid.

[157] ibid., p.54

Recommendation 8:

The Committee recommends that the Department of Premier and Cabinet and Victoria Police:

(a) Take action to identify examples of "best practice" (benchmarks) in relation to the management of departmental responsibilities relating to the protection of essential services under Part 6 of the *Terrorism (Community Protection) Act 2003* and the protection of the Victoria's critical infrastructure; and

(b) Disseminate these "best practice" models to other government departments with critical infrastructure responsibilities to assist with the improvement of critical infrastructure protection management systems and processes across the public sector.

4.4.4 Guidance on identification of essential services for declaration under the Act

As stated earlier, Victoria's approach to critical infrastructure protection is influenced by the events surrounding the Esso Longford Gas crisis in 1998, the rise of the threat of terrorism following the September 2001 attacks and the fact that a significant proportion of the State's essential services and critical infrastructure are either privately owned or operated.

The intention of Part 6 in the *Terrorism (Community Protection) Act 2003* is to provide a higher degree of assurance that the owners/operators of Victoria's essential services have taken steps to prepare for the occurrence of a terrorist incident. The CIP policy Framework followed later in 2007 to seek some assurance through persuasion that other "less critical" infrastructure would be similarly protected against terrorist threat.

As noted, under the Act, the "relevant Minister" as designated by the Premier, is responsible for recommending that an essential service be "declared" for the purposes of the Act. The Act however, is non-prescriptive in defining what constitutes an essential service.

With regard to the implementation of the provisions of Part 6 of the Act, the Auditor-General found that, in order to provide better assurance in terms of completeness of coverage, there was a need for more definitive guidance to assist in determining exactly what constitutes an essential service for declaration under the Act.[158]

The Auditor-General recommended that the DPC provide definitive guidance on identifying essential services for declaration to better inform relevant departments in the discharge of their responsibilities under Part 6 of the Act (Recommendation 4.4).[159]

Response by the Department of Premier and Cabinet

The response provided by the Department in the Minister for Finance Report stated that the definition of "essential services" underpinning the arrangements in place is specified in the 2002 *Review of the Security of Supply of Essential Services*. The DPC noted that the Auditor-General had found that the three most critical sectors had been effectively declared and managed and that this demonstrated that the declaration process was working effectively.

[158] ibid., p.12

[159] ibid., p.41

Further, the DPC responded that the recommendation would be considered as part of the Department's review of the CIP arrangements.[160]

Subsequent developments noted by the Committee

At the public hearing, the Committee was interested in the process of designation under Section 27 of Part 6 of the Act from the Premier to the relevant department and delegations under Section 27A from the relevant Minister to a public servant.

With regard to the role of the Premier in relation to Part 6 of the Act, the DPC advised:[161]

> *…on this point of accountability, I think it is important to understand the distinctly limited role of the Premier under part 6 of the Act. The role of the Premier under Part 6 is basically limited to designating the relevant Minister in respect of an essential service. Once the Premier has done that the rest of Part 6 is all about what the relevant Minister must do or cause to be done.*

The Committee sought to determine whether the DPC had an understanding or record of whether these delegations had been exercised and whether current office holders were aware of these delegations and their responsibilities under the Act.[162]

The Deputy Secretary, DPC advised the Committee that:[163]

> *It is not the DPC's practice or, I would suggest, role to track all of those.*

The Committee considers that these comments, provided in evidence to the Committee, highlight the key issues under review, and that is, determining exactly where responsibility and accountability rests for oversight of the CIP arrangements.[164]

The Chairman requested that details of the delegations made under Part 6 of the Act be advised to the Committee in writing at a later date.

In October 2011, the Department advised the Committee that three departments had made delegations under Section 27A of the Act. The following details were provided by the Department:[165]

[160] Department of Treasury and Finance, *Response by the Minister for Finance to the Auditor-General's Reports issued during 2008-09*, December 2009, p.104

[161] Mr D. Speagle, Deputy Secretary, Federalism, Citizenship and Climate Change, Department of Premier and Cabinet, transcript of evidence, Session 2, 25 August 2011, p.8

[162] Mr P. Davis MP, Chairman, Public Accounts and Estimates Committee, transcript of evidence, Session 4, 25 August 2011, pp.2-3

[163] Mr D. Speagle, Deputy Secretary, Federalism, Citizenship and Climate Change, Department of Premier and Cabinet, transcript of evidence, Session 4, 25 August 2011, p.3

[164] Mr P. Davis MP, Chairman, Public Accounts and Estimates Committee, transcript of evidence, Session 4, 25 August 2011, p.3

[165] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 20 October 2011, pp.1-2

Table 4.1: Delegations made under Part 6 of the *Terrorism (Community Protection) Act 2003*

Department/section	Date of delegation	Status	Proposed action
DOT – Roads	27 February 2008	Revoked and replaced 14 May 2010.	Intended that the delegation will be revoked and made to nominated positions rather than individuals.
DOT – Ports	27 February 2008	Remains in place.	No further action.
DOT – Public Transport	25 February 2008	Revoked and replaced 10 April 2010. Revoked and replaced 20 June 2011 to nominated positions.	Persons affected by delegation are emailed with a copy of the delegation and to confirm their responsibilities and powers under the delegation.
DPI (Energy)	16 April 2008 to officers in DOT	Current	DPI is preparing to revoke this delegation and replace with delegations to nominated positions within DPI.
DSE	29 July 2009	Delegations are current. They were made to nominated positions.	Relevant staff are briefed annually or when staff changes occur.

Source: Table prepared by PAEC Secretariat based on information provided by the Department of Premier and Cabinet, letter to the Committee, received 20 October 2011, pp.1-2

The Department states that the information provided shows that while departments adopt varying approaches to delegations:[166]

> *...all departments have appropriately discharged their responsibilities in informing relevant delegates, keeping these delegates informed of their responsibilities, and ensuring that lessons learnt are appropriately applied (i.e. by delegating to position titles rather than nominated individuals). It is intended that the CGRC adopt a common policy framework for delegations under Part 6, including advice to delegates about their powers and responsibilities.*

Committee findings and recommendation

In terms of declared essential services under Part 6 of the Act, the Auditor-General's report noted that, at the time of the audit, 39 essential services had been declared under the Act. The Committee heard evidence from Victoria Police that it oversees 39 exercises each year to test the operation of the risk management plans of declared essential services.[167]

The DPC advised the Committee that it had sought the assistance of the Victorian Managed Insurance Authority (VMIA) in developing a framework for the identification of critical infrastructure. It is intended that this classification framework will be used by the SCN-CG to develop a methodology to assist the identification of declared essential services however this cannot be finalised until testing and validation of the classification framework is complete.[168]

[166] ibid., p.3

[167] Mr S. Fontana, Assistant Commissioner, Victoria Police, transcript of evidence, Session 3, 25 August 2011, p.4

[168] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.11

At the hearing Assistant Commissioner Fontana indicated that the classification framework tool had been trialled and was now in the process of being rolled out but it was likely to take around 18 months to review the complete list of critical infrastructure (including essential services) already identified to verify their classification and continuing relevance to the State's critical infrastructure register.[169]

Extensive discussion took place at the public hearing with representatives of the DPC and Victoria Police concerning the need for distinctions in terminology between essential services and critical infrastructure. This issue is discussed further in Section 5.2 of this report.

The Committee notes the information provided by the DPC in respect to delegations made under Part 6 of the Act and the intention of the CGRC to seek a "common policy framework" to be applied to such delegations. The Committee considers that the approach should seek to ensure that processes are in place to regularly review delegations to ensure that they remain current and relevant. Processes should also include regular briefings and refreshers for delegated officers to ensure that requirements under the delegations are clearly understood and that knowledge and awareness of the requirements of the Act are maintained.

Recommendation 9:

The Committee recommends that the Department of Premier and Cabinet proceed with its intention to formalise and standardise the delegation process by relevant departments under Section 27A of Part 6 of the *Terrorism (Community Protection) Act 2003* to ensure that departments adopt a common process for ensuring delegates are fully aware of their powers and functions under the Act and that a process is in place to regularly review delegations to ensure they remain relevant and appropriate.

4.4.5 Inter-agency risk management

The Auditor-General's report notes that when departments work across their departmental boundaries in a coordinated or "joined-up" way, it is important that any risks and/or opportunities associated with these arrangements are identified and managed to ensure that they do not detract from effective policy implementation, service delivery or the achievement of objectives. The Auditor-General refers to this type of risk as "inter-agency risk".[170]

Some of the risks he identified in his report were:[171]

- a lack of clearly defined goals to promote a shared understanding between the parties involved;
- poor communication between agencies;
- inadequate resources;
- a lack of clear and proactive leadership; and

[169] Mr S. Fontana, Assistant Commissioner, Victoria Police, transcript of evidence, Session 3, 25 August 2011, pp.12-13

[170] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.34

[171] ibid., p.35

- unclear identification of roles and responsibilities.

The Auditor-General commented that risk management planning should include consideration of the impact of these types of risks together with strategies to mitigate them.

The Auditor-General found that there was little evidence to indicate that agencies involved in implementing Part 6 of the Act and the CIP policy Framework had identified and managed inter-agency risks.[172]

The Auditor-General recommended that the DPC identify risks arising from the "joined-up" nature of the arrangements in place for the protection of essential services and critical infrastructure and assist the relevant lead departments and agencies in the development of associated risk management arrangements at the whole-of-government level (Recommendation 4.5).[173]

Response by the Department of Premier and Cabinet

The response provided by the Department in the Auditor-General's report stated that the recommendation and its intent would be considered as part of its review of the CIP arrangements.[174]

Subsequent developments noted by the Committee

Correspondence to the Committee from the DPC in June 2011 noted:[175]

> *Any risks identified by industry and government departments will be reviewed as appropriate by the Security and Continuity Networks Coordination Group.*

The Committee noted that the DPC Review Report did not contain any recommendations addressing the management of "inter-agency risks" however mention was made of the importance of managing "dependent risk" between industry sectors.[176]

At the public hearing in August 2011, the Secretary of the DPC agreed that there are special risks associated with interdependent and dependent sectors that need to be considered by government in order to ensure appropriate risk management.[177]

The Secretary gave evidence to the Committee that the issue of interdependency between critical infrastructure industry sectors had been gaining prominence and Victoria Police and a number of SCNs had looked at conducting joint exercises between sectors to raise awareness of the issues of interdependent and dependent risk. The "All-Forums" meeting in

[172] ibid.

[173] ibid., p.41

[174] Department of Treasury and Finance, *Response by the Minister for Finance to the Auditor-General's Reports issued during 2008-09*, December 2009, p.104

[175] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, Attachment C, received 17 June 2011

[176] Department of Premier and Cabinet, *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure*, 15 June 2011, pp.7-8

[177] Ms H. Silver, Secretary, Department of Premier and Cabinet, transcript of evidence, Session 2, 25 August 2011, p.9

February 2011, which included around 100 industry and government stakeholders, also looked at these issues and how to progress risk management in this area.[178]

Following the public hearing the Committee requested further detail from the DPC as to what specific action had been taken by the Department to identify the risks associated with the joined-up nature of CIP arrangements and to assist relevant government agencies to develop comprehensive risk management planning.

The DPC advised that it considers "inter-agency" or "joined-up" risk *"to be a subset of dependent risk, particularly focussed on the interactions between government agencies."*[179] Information provided by the Department indicated that interagency risks are considered as follows:[180]

- through discussion at critical infrastructure forums such as the SCN-CG and the CGRC;
- the NCTC's *National Guidelines for Protecting Critical Infrastructure from Terrorism* provide for collaboration between the Commonwealth and the states and territories to *"identify critical infrastructure and over time provide information on interdependencies"*;
- recent participation by DPC officers in Commonwealth government workshops specifically focussed on managing dependent risk;
- one of the corporate risks identified in the DPC's overall risk management strategy relates to the management of inter-departmental consultation and collaboration. This risk is managed by Branch Directors who seek to: identify opportunities for cross-departmental collaboration; establish and implement a stakeholder management strategy for effective engagement of government and non-government bodies; and improve governance and accountability structures relating to whole-of-government initiatives; and
- work undertaken by the DTF on the development of a State-wide risk register. The register was compiled through a series of seminars conducted by the VMIA across government agencies with senior representation from the DPC. The risk of a major terrorist attack was considered by participants as part of this process.

Committee findings and recommendations

The Committee notes that the *Victorian Government Risk Management Framework*, issued by the Department of Treasury and Finance, states that the management of risk is an important component of public sector governance and that an agency's approach must be consistent with the *Australian/New Zealand Risk Management Standard ISO 31000:2009*, directions under the *Financial Management Act 1994* and the *Victorian Government Risk Management Framework.*[181]

[178] ibid., p.10

[179] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 20 October 2011

[180] ibid., pp.11-12

[181] Department of Treasury and Finance, *Victorian Government Risk Management Framework*, March 2011, p.3

The Framework notes that risks can be categorised in many ways and are generally broken into financial risks and non-financial risks. Non-financial risks include a range of categories such as: strategic risks (e.g. strategic planning; governance; emergencies; energy/water security; etc.); operational risks (e.g. infrastructure; OHS; public health and safety; etc.); people management risks; environmental risks; knowledge and system management risks; legal and reputational risks.[182]

The Risk Management Framework also refers to interagency and state-wide risks as follows:[183]

> *In addition to managing agency risks, the Framework also emphasises the need to address interagency and statewide risks when developing and implementing risk management frameworks and processes. Increasingly the public sector is operating in an environment of shared accountabilities to achieve outcomes that cut across specific departmental responsibilities. In this context it is important that risks with the potential to impact across agencies or at a whole of government level are communicated or escalated to potentially affected agencies to enable a coordinated, effective and timely approach to risk management.*

This reference to the identification and management of state-wide risks is particularly pertinent to risk management in the area of critical infrastructure protection particularly where interdependencies between sectors have been identified and also in relation to the management of emergency response and recovery efforts in the event of an incident.

In relation to accountability for risk management, the *Victorian Risk Management Framework* states that a number of agencies play a key role in monitoring, reporting and advising government in relation to compliance with risk management requirements under existing legislation, and risks that impact more broadly across the public sector.

The Committee notes that under the *Victorian Risk Management Framework*, the DPC has a pivotal role in state-wide risk management through coordination of the Cabinet process and support of the Premier on government-wide issues, as well as in his portfolio of ministerial responsibilities. This includes minimising risk through:[184]

- advising the Premier on policy issues, with briefings typically including advice on key risks relating to an issue, including because of action or inaction;
- analysing whole-of-government governance and risk issues;
- coordinating whole-of-government policy and position on particular matters; and
- providing checks and balances through the Cabinet cycle.

The Committee considers that, as the administrator of Part 6 of the Act and the agency responsible for the oversight of critical infrastructure protection policy in the State, the DPC has an important role to play in ensuring that inter-agency risks associated with the application and implementation of critical infrastructure protection legislation and policy have

[182] ibid., p.25

[183] ibid., p.4

[184] ibid., p.9

been identified and are considered as part of the Department's risk management planning processes.

In addition, the Department's critical infrastructure risk management strategy should also take into consideration the impact on desired policy outcomes of central agency management risks, such as:

- the lack of direction and strong leadership;
- the lack of appropriate capability (i.e. systems for costing and performance information, management development, etc);
- a lack of detailed and appropriate documentation and information available to demonstrate to the Parliament and the public that policy objectives and legislative requirements have been met; and
- difficulty in implementing performance assessment and benchmarking to demonstrate the effectiveness of the arrangements in place.

Some of the issues identified in the Auditor-General's report and confirmed by this Committee relate to the management risks outlined above.

Recommendation 10:

The Committee recommends that the Department of Premier and Cabinet ensure that inter-agency and state-wide risks associated with the implementation of critical infrastructure protection arrangements in the State are identified as a part of the Department's risk management planning processes and that appropriate strategies are developed to manage those risks.

Recommendation 11:

The Committee recommends that the Department of Premier and Cabinet's risk management approach, in relation to its central oversight of critical infrastructure arrangements, takes into consideration any risks associated with: poor central oversight and direction; lack of appropriate and relevant performance measurement; and informal and unstructured reporting systems; together with strategies to address those risks.

4.4.6 The Security and Continuity Network structure

The CIP policy Framework called for the establishment of nine sector-based SCNs to provide for communication and consultation between government and industry owners/operators of critical infrastructure. In addition, as mentioned earlier in this Chapter of the report, a SCN-Coordination Group was established to oversee and guide developments in each sector and report to the CGRC.

The Auditor-General found that the operational maturity of the SCNs varied significantly. There were delays in establishing some SCNs and a lack of clarity about whether others were in fact needed. These factors had impacted detrimentally on the SCN structure in providing an effective component of the governance arrangements operating over the protection of the State's critical infrastructure. Specifically there were three SCNs which had not been established: one in the "Banking and Finance" sector; one in the "Communications" sector; and one for "Places of Mass Gatherings".[185]

The Auditor-General recommended that the DPC clarify the requirements with respect to the establishment of SCNs in designated sectors, so that there is a common understanding by the relevant lead departments of those requirements (Recommendation 4.6).[186]

Response by the Department of Premier and Cabinet

The response provided by the Department in the Minister for Finance Report stated that the recommendation in relation to the establishment of SCNs was accepted and would be considered as part of the review of CIP arrangements being undertaken. In addition, the DPC stated that it had led the establishment of the Banking and Finance Security Continuity Network and had taken steps with Victoria Police to progress the establishment of the Communications Security Continuity Network.[187]

Subsequent developments noted by the Committee

The Committee wrote to the Department in May 2011 requesting information on the status of each of the nine SCNs proposed under the CIP policy Framework and also for advice on how the Parliament can be assured that all relevant and appropriate SCNs are now fully operational and are performing their responsibilities effectively.

Establishment of Security and Continuity Networks

The Department advised the Committee that as a result of a review conducted by the Commonwealth Government in 2009, "Places of Mass Gatherings" are no longer considered to constitute critical infrastructure *"as the risks faced by them primarily relate to terrorism rather than being all-hazards based.*" Victoria now complements the National Counter-Terrorism Committee work relating to the risks associated with mass gatherings through the involvement of Victoria Police. As a result there are now eight SCNs covering critical infrastructure protection in the State.[188]

The following table provided by the DPC sets out the current status of the SCNs.[189]

[185] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.31

[186] ibid., p.41

[187] Department of Treasury and Finance, *Response by the Minister for Finance to the Auditor-General's Reports issued during 2008-09*, December 2009, p.105

[188] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.9

[189] ibid., pp.9-10

Table 4.2: Status of critical infrastructure Security and Continuity Networks as at June 2011

SCN (Chair)	Annual meetings	Date of last meeting	Members	Terms of reference established	Notes
Banking & Finance (DPC)	3-4	8 March 2011	13 primary 18 secondary	Yes	n/a
Communications (ESTA)	4	6 May 2011	Approx. 20	Yes	n/a
Energy (DPI)	2	8 December 2010	Approx. 45	Yes	Engaged with other critical infrastructure sectors with dependent on the energy sector.
Food Services (DPI)	2	4 May 2010	Approx. 25 and 10 observers	Yes	Assisted in Black Saturday recovery efforts and recent State floods.
Health[a] (DOH)	3	Not provided	Not provided	Not provided	State Health and Medical Sub-Committee provides a forum for security issues in the health sector.
Police & Emergency Services (OESC)	2	10 May 2011	11	Yes	n/a
Transport (DOT)	4			Yes[b]	The Transport SCN has been split into two SCNs:
Roads, Ports & Freight SCN		10 May 2011	Approx. 20		Roads, Port & Freight; and
Public Transport SCN		17 May 2011	Approx. 25		Public Transport
Water (DSE)	2	6 April 2011	25	Yes	n/a

Source: Department of Premier and Cabinet, June 2011

Notes:

ESTA – Emergency Services Telecommunications Authority

DPI – Department of Primary Industries

DOH – Department of Health

OESC – Office of Emergency Services Commissioner

DOT – Department of Transport

DSE – Department of Sustainability and Environment

(a) The Department of Health and the Department of Human Services assert that they meet the Health SCN objective through the State Health and Medical Sub-Committee.

(b) Use 'Operating Principles' in place of 'Terms of Reference'.

In response to the Committee's question regarding assurance that the SCNs were now fully operational and performing their responsibilities effectively, the DPC advised:[190]

[190] ibid., p.10

> *…all SCNs are now fully operational. While their different aims, membership and levels of engagement with Victorian Government lead to varying levels of development, through the Security Continuity Network-Coordination Group, it is intended that they will ultimately achieve a common standard of maturity.*

The Committee notes that the DPC Review Report comments that although not specifically stated in the CIP policy Framework, there is an ability to establish additional SCNs to address emerging risks, for example, in the information and communication technology (ICT) area. The Report states that a revised CIP policy Framework will include clearer guidelines on how an SCN can be established, disbanded or moved to more appropriate forums.[191]

The DPC Review Report confirmed that a key strength of the CIP arrangements was the industry-government partnerships facilitated through the SCN structure. The Report notes:[192]

> *Although membership of the SCNs is voluntary for industry members, participation has been strong and the information gained valuable. Further, the relationships and networks have delivered additional benefits beyond managing the risks from terrorism including consideration of broader concerns, incident response and emergency management. This was evident during the Black Saturday bushfires, where, for example, the transport sector was able to utilise the government-industry network to enhance their emergency response capability.*

This comment was reinforced by evidence provided at the public hearing where the DPC advised that during the recent floods in Victoria, the DPI used the Food sector SCN to assist in responding to food supply continuity threats in the Kerang area over that time and to facilitate the return of displaced persons once the floodwaters receded.[193]

Update on Banking and Finance, Communications and Health Security and Continuity Networks

The Auditor-General's report noted that the former Department of Innovation, Industry and Regional Development (now the Department of Business and Innovation) considered that SCNs in the "Banking and Finance sector" and the "Communications sector" were inappropriate as these sectors operate under national infrastructure protection arrangements in which the Department of Business and Innovation participate.[194]

Correspondence received from the DPC advised that SCNs in these sectors had since been established. The Committee requested further information on the actions taken by the DPC to establish these SCNs in light of the Department of Business and Innovation refusing to be involved.

[191] Department of Premier and Cabinet, *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure*, 15 June 2011, p.15

[192] ibid., p.10

[193] Mr M.Duckworth, Executive Director, Citizenship and Resilience, Department of Premier and Cabinet, transcript of evidence, Session 2, 25 August 2011, p.10

[194] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.31

The DPC advised that it had established these SCNs together with Victoria Police in response to representations from industry members that there was value in having local networks to facilitate preparedness and response during an emergency. The Department advised that the Emergency Services Telecommunications Authority (ESTA) has a good understanding of communications issues and strong relationships with emergency service organisations so it was considered a natural fit to take over the chairing of the Communications SCN from Victoria Police in May 2011.[195]

In relation to the Banking and Finance SCN, the DPC continues to chair this network however the Department advised that the VMIA has indicated a willingness to take on the chairing role when resources permit. The Department considers that the VMIA's understanding of the issues and relationships within the insurance and finance industries make it an appropriate leader for the Banking and Finance SCN.[196]

The Auditor-General's report noted that the Department of Health (DOH) had advised that it had not actively communicated the CIP policy Framework in the "health sector" as it did not believe the sector would *"respond favourably to counter-terrorism initiatives"* as it had a focus on "all-hazards" in its emergency management preparedness.[197]

Correspondence provided by the DPC in June 2011 in relation to the establishment of SCNs advised that the management of State security issues impacting the health and human services sector are handled through the State Health and Medical Sub-Committee and that one of this Sub-Committee's primary tasks in 2011 is to identify critical infrastructure in the health sector in conjunction with Victoria Police.[198]

The Committee followed this matter up with Victoria Police to ascertain whether they considered the current SCN arrangements adequate particularly as they relate to the identification of critical infrastructure sites in the health sector. The DOJ advised that SCNs cover both declared essential services and critical infrastructure however there is no requirement on owners/operators of either to participate and, in fact, some do not participate in this activity.[199]

Further, in relation to the health sector, advice received by Victoria Police was that significant natural disasters in Victoria in recent years had delayed engagement and commitment to a SCN in this sector. Also Victoria Police has been advised by the health sector that current redundancy arrangements would meet most if not all emergency situations. The CIPU, Victoria Police had briefed the Secretaries of both the Department of Health and the Department of Human Services on their responsibilities and the State Health and Medical Sub-Committee was continuing to engage with the CIPU to progress this issue of critical infrastructure identification and protection. The DOJ commented that:[200]

[195] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 20 October 2011, p.18

[196] ibid.

[197] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.30

[198] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.10

[199] Ms P. Armytage, Secretary, Department of Justice, letter to the Committee, received 13 October 2011, p.3

[200] ibid., p.5

> *The present arrangements are not totally adequate, but Victoria Police is working with the health sector and expect to continue further discussions shortly.*

The DOJ advised the Committee that a number of critical infrastructure sites in the health sector were already on the jurisdictional list of Victoria Police and it was proposed to use the new critical infrastructure evaluation tool and health sector expertise to identify any additional sites however this was expected to be small given the current redundancy arrangements.[201]

Committee findings and recommendations

Based on the review of the documentation made available to the Committee and evidence provided to the Committee at the hearing, the Committee acknowledges that SCNs in the transport, water and energy sectors are well established and operating effectively as intended.

In relation to the other SCNs, the Committee wishes to express some concern over the apparent lack of commitment on the part of the Department of Health, the Department of Human Services and the Department of Business and Innovation in supporting the State's CIP policy Framework and local industry groups within their portfolios.

The Committee notes the existence of the State *Health Emergency Response Plan* (SHERP) *Victoria* which is a detailed and comprehensive sub-plan of the *Victoria State Emergency Response Plan*. SHERP adopts an "all hazards" approach with the principles outlined in the plan applying to any emergency (regardless of cause) including at mass gatherings and public events and covers:[202]

- mass casualty incidents;
- complex trauma emergencies;
- chemical, biological or radiological incidents;
- food and drinking water contamination involving health impacts;
- human illness epidemic;
- natural disasters; and
- disruption to essential services.

While the Committee accepts the explanation from the Department of Health, via the DPC, that the health sector emergency management focus is on "all hazards" and not just the threat of a terrorist incident, it is concerned that the identification of critical infrastructure in the sector has not been undertaken, for example, the storage and/or location of medical supplies such as vaccines and antibiotics. The Committee notes also that one of the express "operating principles" of the SCN-CG is to ensure that critical infrastructure in Victoria is adequately identified, critically determined and ranked.[203] The Committee found that the SCN-CG has

[201] ibid.

[202] Department of Health, *State Health Emergency Response Plan (SHERP Victoria)*, Version 2, 2009, p.1

[203] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.27

been remiss in this area and the Department of Health does not consider compliance with the Government's CIP policy Framework as a high priority.

Recommendation 12:

The Committee recommends that the Department of Health make it a priority to identify a complete list of Victoria's health sector critical infrastructure and take action to ensure that procedures are in place to protect this infrastructure from all identifiable threats and risks.

Recommendation 13:

The Committee recommends that the Security and Continuity Network-Coordination Group take action to ensure that all critical infrastructure sites in the Victorian health sector are identified and that appropriate risk management strategies are in place to protect those sites.

Recommendation 14:

The Committee recommends that the Security and Continuity Network-Coordination Group take action to include the Department of Health in discussion and sharing of information to assist in the security and risk management protection of critical infrastructure sites in the health sector.

4.4.7 Effectiveness of the Security and Continuity Network-Coordination Group

In addition to commenting on the establishment of SCNs, the Auditor-General reviewed the activities of the SCN-CG and noted that the effectiveness of the Group could be improved by:[204]

- clarification of the co-chairing roles of the DPC and Victoria Police;
- development of a plan outlining the Group's objectives, strategies and milestones together with monitoring processes for implementation of the plan;
- development of a timetable for implementation of the CIP policy Framework with progress reports required from relevant departments/agencies;
- expansion of its oversight and guidance role to include application of Part 6 of the Act;
- providing clarification of the critical infrastructure protection responsibilities of lead departments; and
- providing guidance on specific terminology used in the CIP policy Framework and in Part 6 of the Act to assist in standardising interpretation and application.

[204] ibid., p.28

The Auditor-General did not include a specific recommendation to address the effectiveness of the SCN-CG however the observations made in his report have been followed up by the Committee as part of its Inquiry.

The DPC Review Report noted concerns about the role and objectives of the SCN-CG. The Report states that these concerns could be addressed by incorporating a more definitive role for the SCN-CG in the revised CIP policy Framework to ensure that it provides strategically focussed leadership, support and reporting lines. In addition, the Review Report proposed that the Group's Terms of Reference should be re-examined to ensure it gains appropriate senior level membership and sponsorship.[205]

As noted earlier in this Chapter, at the public hearing in August 2011 the Secretary, DPC identified the role of the Department in its co-chairing of the SCN-CG and in the chairing of the CGRC as the main methods by which the DPC exercises its oversight responsibilities in relation to Part 6 of the Act and in relation to the CIP policy Framework. The Secretary acknowledged that there were different levels of maturity across the SCNs and that it was an area which required some strengthening. The Secretary stated at the hearing:[206]

> *One of the key aims of the network is for all these Security and Continuity Networks to achieve the same level of maturity. It is understandable why transport and water is so mature, and they provide the benchmarks for other security networks. The reason transport and water is more mature is that they have very committed industry members, they have a much longer history in this space because of the nature of terrorist risks in these areas, which is well documented, they have strong commitment and reporting process. We wish to see that across all the networks; we are not saying it is there yet.*

Subsequent to the public hearing, the Committee requested further details from the DPC about the enhancements planned to strengthen the SCN-CG and improve oversight by this Group.

The Department advised that since the Auditor-General's report, the SCN-CG has developed a three year Strategic Plan which aims to develop:[207]

- knowledge management;
- resilience to major infrastructure failure;
- understanding of cyber risks; and
- maturity and best practice.

In addition the Group's Terms of Reference have been amended to encompass "resilience" and an "all-hazards" approach in line with COAG's *National Disaster Resilience Strategy* and the Australian Government's *Critical Infrastructure Resilience Strategy*, with individual SCNs to follow with similar amendments to their terms of reference.[208]

[205] Department of Premier and Cabinet, *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure*, 15 June 2011, p.12

[206] Ms H. Silver, Secretary, Department of Premier and Cabinet, transcript of evidence, Session 2, 25 August 2011, pp.7-8

[207] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 20 October 2011, p.13

[208] ibid.

The revised CIP policy Framework will take into consideration issues raised in the DPC Review Report in relation to the perceived limitations of the SCN-CG. The revised policy will also clarify the co-chairing arrangements of the Group by the DPC and Victoria Police. Finally the Department advised that in developing a revised CIP policy Framework, the DPC in consultation with other departments will determine whether the SCN-CG provides the most appropriate body to manage the needs of declared essential service operators and their portfolio departments or whether a different forum or arrangement is better suited.[209]

Committee findings and recommendations

The CIP policy Framework establishes the SCNs and the policy states that these *"will form the heart of the Victorian CIP management arrangements."* Further, each of the lead departments, in consultation with the DPC were to determine the most appropriate membership and method of engagement best suited to the needs and priorities of each sector.[210]

In relation to the role of the SCN-CG (co-chaired by DPC and Victoria Police), the Committee notes that the CIP policy Framework states:[211]

> *This group will oversee and provide guidance on CIP major developments in each sector and report to the CGRC. It will provide each critical infrastructure sector with access to government's senior executives to facilitate the resolution of concerns and assist, where possible, in the development of significant critical infrastructure protection initiatives.*

Based on the role outlined in the CIP policy Framework and the operating principles of the SCN-CG as outlined in the Auditor-General's report, the Committee is unclear and alarmed as to why this coordinating committee has not been more proactive and diligent in performing its responsibilities in the past.

The Committee concludes that the effectiveness of the SCN-CG since its inception in April 2007 appears to be somewhat less than satisfactory given that:

- it is only recently that SCNs have been established in the Banking and Finance sector and in the Communications sector;
- critical infrastructure in the Health sector is yet to be identified; and
- the oversight of the operations and effectiveness of SCNs generally has been limited.

Evidence received by the Committee indicates that the DPC has placed and continues to place a heavy reliance for governance and accountability over the State's CIP arrangements in the committee structure developed under the CIP policy Framework.

[209] ibid., p.14

[210] Victorian Government, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007, p.14

[211] ibid., p.15

Of some concern to the Committee is that the DPC has noted that in its revision of the CIP policy Framework, the SCN-CG may not even be the most appropriate forum for monitoring the application of Part 6 of the Act or for providing leadership in the management of risks relating to critical infrastructure in the State.[212]

Given that the Department has indicated that *"the revised Critical Infrastructure Protection Framework will be developed in the course of 2012"* but not issued until early to mid 2013 it seems apparent to the Committee that significant action will need to be taken to improve the effectiveness of the SCN-Coordination Group in the interim, particularly in relation to its guidance and monitoring responsibilities.[213]

Recommendation 15:

The Committee recommends that the Security Continuity Network-Coordination Group should be more diligent in carrying out its responsibilities with regard to ensuring that the Security and Continuity Networks are operating effectively and as intended and that the Auditor-General review its diligience and effectiveness over the next two years.

Recommendation 16:

The Committee recommends that the Security Continuity Network-Coordination Group seek to identify "best practice" Security and Continuity Networks in an effort to highlight practices and activities which might be adopted in those less well developed Networks.

4.4.8 Role of the Central Government Response Committee in monitoring the Security and Continuity Network structure

Correspondence from the DPC in June 2011 indicated that it was intended that the CGRC would take increased responsibility in overseeing the work of the SCN-CG which will enable the latter to seek formal reports from SCNs and provide greater assurance to Government that these networks are operating effectively.[214]

The DPC Review Report recommends that the CGRC actively oversight the work of the SCN-CG through appropriate tasking and minimum annual reviews of the work of the SCN-CG.[215]

It is interesting to note that advice provided by the DPC indicates that the CGRC meets more regularly (every two months) than the SCN-CG (every three months).[216]

[212] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 20 October 2011, p.8, p.14

[213] ibid., p.19

[214] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.11

[215] Department of Premier and Cabinet, *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure*, 15 June 2011, p.12

[216] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 20 October 2011, pp.8-9

At the hearing, Assistant Commissioner Fontana from Victoria Police advised the Committee that he was of the view that any significant issues or problems identified during their supervision of declared essential services exercises under Part 6 of the Act would be reported to the CGRC.[217]

In relation to critical infrastructure monitoring arrangements where there is no statutory requirements in place, Asssitant Commissioner Fontana advised the Committee that much of the training and capability building occurred at the local level with local police and local emergency services personnel working with critical infrastructure operators. In this instance the SCNs would provide the forum for information sharing and reporting in relation to these arrangements.[218]

The Auditor-General's representative, Ms Ellen Holland, Assistant Auditor-General, Financial Audit, expressed concern at the hearing that the evidence obtained at the time of the audit showed a lack of coordination at the CGRC level and that the SCN-CG was more concerned with critical infrastructure arrangements under the CIP policy Framework rather than declared essential services under Part 6 of the Act which raised questions about the focus or emphasis of issues during committee meetings.[219]

In response to these concerns, Assistant Commissioner Fontana stated: [220]

> *…We have certainly changed the level of representation that we have on that coordination committee, and it is far more focussed…and I think they have come a long way.*
>
> *…You will never get a perfect system, but the reporting does go up through that particular network. It is evolving. All these systems…are always being looked at and we are self-assessing, identifying gaps and working on them… But in terms of the security and continuity network that is where we push it up to CGRC. There is no regulatory requirement for that to exist; it is a Framework. There is a lot of goodwill among the players and operators within those particular networks.*

During the joint hearing with representatives from both the DPC and the DOJ further evidence was provided to the Committee by the DPC that the reporting arrangements between the SCN-CG and the CGRC had become clearer and more formalised over the past 12 months than they were at the time of the Auditor-General's review.[221]

Committee findings and recommendation

[217] Mr S. Fontana, Assistant Commissioner, State Emergencies and Securities Department, Victoria Police, transcript of evidence, Session 3, 25 August 2011, p.13

[218] ibid., p.14

[219] Ms E. Holland, Assistant Auditor-General, Financial Audit, Auditor-General's Office, transcript of evidence, Session 3, 25 August 2011, pp.14-15

[220] Mr S. Fontana, Assistant Commissioner, State Emergencies and Securities Department, Victoria Police, transcript of evidence, Session 3, 25 August 2011, p.15

[221] Mr M. Duckworth, Executive Director, Citizenship and resilience, Department of Premier and Cabinet, transcript of evidence, Session 4, 25 August 2011, pp.8-9

The Committee notes that the Auditor-General's recommendations were directed at strengthening oversight by the DPC itself and also through an expansion in the terms of reference of the SCN-CG to include declared essential services (and therefore Part 6 of the Act) in their oversight.

The DPC advised the Committee that the terms of reference of the SCN-CG have been amended to embrace the concept of "resilience" and now state the Group's purpose as:[222]

> *…provide strategic guidance and leadership to identified critical infrastructure sectors to enhance resilience. This will include providing essential service operators and critical infrastructure sectors with access to senior government executives to facilitate the resolution of concerns and assist, where possible, in the development of critical infrastructure resilience initiatives.*

The Committee acknowledges advice provided by the DPC in relation to the plans to strengthen the reporting arrangements between the SCN-CG and the CGRC. The Committee also notes advice from the DPC that the role and structure of the CGRC will be considered as part of the Green paper review *Towards a More Disaster Resilient and Safer Victoria*.[223]

It is the Committee's view that of greater importance, in terms of the monitoring and oversight of critical infrastructure protection arrangements in the State, is the need for strengthening and formalising the reporting arrangements between the SCNs and the SCN-CG. This in turn should provide benefits in terms of the quality of reporting from the SCN-CG up to the CGRC.

Recommendation 17:

The Committee recommends that the reporting arrangements in place between the Security and Continuity Networks and the Security Continuity Network-Coordination Group be improved to provide more regular and standardised reports on the status of the key issues relating to the protection of critical infrastructure in the State such as: the identification and recording of sites; the status of risk management arrangements and business continuity planning; and emergency training.

4.4.9 Security clearances

The Auditor-General recommended that representatives of lead departments should obtain the necessary security clearances to allow access by appropriate officers to relevant and pertinent information to assist planning, management and decision making within their sectors (Recommendation 4.7).[224]

[222] ibid., p.8

[223] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 20 October 2011, p.9

[224] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, pp.38, 41

Response by departments

The DPC stated in the Minister for Finance Report that this recommendation was strongly supported and that members of the Central Government Response Committee had been reminded of their departments' obligations to ensure security clearances are obtained for the appropriate personnel.[225]

The responses provided by each of the lead departments in the Minister for Finance Report supported the Auditor-General's recommendation and stated that appropriate action had been taken to address any deficiencies in enabling appropriate officers to obtain access to information required.

Committee finding

The Committee found that this recommendation has been addressed satisfactorily and no further follow-up is required.

[225] Department of Treasury and Finance, *Response by the Minister for Finance to the Auditor-General's Reports issued during 2008-09*, December 2009, p.105

CHAPTER 5: RISK MANAGEMENT AND COMPLIANCE

5.1 Introduction

Part of the Auditor-General's audit involved a review of how Victoria Police and the relevant government agencies managed compliance with the legislation and the *Victorian Framework for Critical Infrastructure Protection from Terrorism* (CIP policy Framework).

Part 6 of the *Terrorism (Community Protection) Act 2003* (the Act) mandates for the operators of "declared essential services" to prepare risk management plans to identify and mitigate the risk of terrorist acts.[226] The current CIP policy Framework establishes guiding principles and coordination arrangements for government agencies and industry to jointly develop strategies to protect Victoria's critical infrastructure from terrorism. The policy recommends that all owners/operators of identified critical infrastructure adopt similar risk management procedures to those prescribed in the Act for declared essential services.

5.2 Identifying essential services and critical infrastructure

The Act and the CIP policy Framework each refer to different terminology that substantially relates to similar things. The Act refers to essential services as including transport, water, fuel, light, power, sewerage and any other service declared to be an essential service by the Governor-in-Council.[227]

Under the CIP policy Framework:[228]

> *Critical infrastructure consists of those physical facilities, supply chains, information technologies and communication networks which, 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.*

In addition, the CIP policy Framework describes "declared essential services" as those services that are indispensable to maintain the safety and well-being of the population at all times.

Under the Act, "relevant Ministers" (through their departments) are responsible for the identification of essential services under their department's purview or for any other assets or services which should be declared as an essential service for the purposes of the Act. An essential service, or part of an essential service, only becomes a declared essential service where the "relevant Minister" has provided the owner/operator with a copy of the Order by the Governor-in-Council.[229]

Under the CIP policy Framework the responsibility for the identification and prioritisation of the State's critical infrastructure and for the maintenance of the Victorian critical infrastructure register is conferred on Victoria Police.[230]

[226] *Terrorism (Community Protection) Act 2003*, s. 1(d)

[227] ibid., s. 26

[228] Victorian Government, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007, p.6

[229] ibid., p.9

[230] ibid., pp.8-9

Neither the Act, nor the CIP policy Framework, contain criteria to assist departments and Victoria Police in the identification and prioritisation of critical infrastructure.

5.2.1 Auditor-General's findings and recommendations

The Auditor-General examined how Victoria Police and the six government departments had identified essential services and critical infrastructure across the nine industry sectors.

Of the lead departments reviewed, the Auditor-General observed that:

- the Department of Sustainability and Environment (DSE) and the Department of Transport (DOT) had both been proactive in developing a method to identify essential services. This had resulted in 39 essential services being declared in the water, energy and transport sectors at the time of the audit;[231]

- the Department of Justice (DOJ) had not formally "declared" essential services in the "Police and Emergency Services" sector as regular testing of emergency services forms a normal part of the sector's operations;[232] and

- the remaining departments – the Department of Health (DOH), the former Department of Innovation, Industry and Regional Development (DIIRD) and the Department of Primary Industries (DPI) – had not declared any essential services in their respective industry sectors. As such the Auditor-General was unable to ascertain whether all of Victoria's essential services had been identified and declared.[233]

The Auditor-General noted at the time of the audit, that 256 critical infrastructure sites had been registered by Victoria Police.[234] In relation to identifying critical infrastructure under the CIP policy Framework, the Auditor-General found that:

- in a number of instances, lead departments were unaware of the registered sites in the sectors under their purview and this had restricted their ability to work with the owners/operators. Also there were no processes in place to enable these lead departments to access information contained in the critical infrastructure register maintained by Victoria Police;[235] and

- three departments (DOH, DIIRD and DOJ) were not actively engaged in identifying critical infrastructure within their sectors. DIIRD viewed their relevant industry sectors as coming under national jurisdiction and DOH and DOJ adopt an "all hazards, all agencies" approach to emergency management.

The view of the DOH was that the health sector managed for all threats and hazards and therefore communication regarding protection from terrorism was seen as unnecessary. In the case of the DOJ, it also advised that it managed on an all hazards, all agencies approach as directed in the *Victoria State Emergency Response Plan* and the *Emergency Management*

[231] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.46

[232] ibid.

[233] ibid., p.47

[234] ibid.

[235] ibid., pp.47-8

Manual Victoria and that the CIP policy Framework was seen as interfacing with those arrangements.[236]

Finally, the Auditor-General found that there was some overlap between declared essential services and registered critical infrastructure and that Victoria Police were planning to review the register to assess whether all sites should, in fact, be registered.[237]

The Auditor-General recommended that the DPC and Victoria Police work together to develop clear guidance to assist departments, Victoria Police and owners/operators in distinguishing between declared essential services and critical infrastructure (Recommendation 5.1).[238]

5.2.2 Responses by the Department of Premier and Cabinet and the Department of Justice

The response of the Department of Premier and Cabinet (DPC) in the *Response by the Minister for Finance to the Auditor-General's Reports 2008-09* (Minister for Finance Report) stated that the intent of the recommendation would be considered in the review of the Critical Infrastructure Protection (CIP) arrangements being undertaken. The response also stated that the DPC had supported Victoria Police in establishing a project to review the risk management methodology applied to identify critical infrastructure for registration and that the project was due to be finalised by the end of 2009.[239]

The response of the DOJ as provided in the Minister for Finance Report stated that the recommendation would be implemented by the DPC and Victoria Police.[240] No further details as to the action proposed to address the recommendation was provided in the response.

5.2.3 Subsequent developments noted by the Committee

Actions taken to clarify definitions

The Committee wrote to both the DPC and the DOJ in May 2011 requesting an update on the actions taken by the departments to clarify the differences between declared essential services and critical infrastructure.

The DPC advised that during 2010, with the assistance of the Victorian Managed Insurance Authority (VMIA), it had developed the *Victorian Infrastructure Classification Framework* which it stated is managed by Victoria Police. The DPC advised also that the Classification Framework was validated by Victoria Police and relevant agencies during the first quarter of 2011 to ensure accuracy and reliability and is now being distributed to other agencies for trial and implementation across government.[241]

[236] ibid., p.48

[237] ibid.

[238] ibid., p.59

[239] Department of Treasury and Finance, *Response by the Minister for Finance to the Auditor-General's Reports issued during 2008-09*, December 2009, p.105

[240] ibid., p.64

[241] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.11

Further, with regard to declared essential services, the DPC advised that members of the Security and Continuity Network-Coordination Group (SCN-CG) have developed a methodology to determine declared essential services based on the *Victorian Infrastructure Classification Framework*. The DPC advised that, once the testing of the Classification Framework is complete, the methodology for determining declared essential services will be finalised and the Auditor-General's recommendation will have been actioned.[242]

The DOJ responded to the Committee in June 2011 that work on definitions to distinguish between critical infrastructure and declared essential services had been developed but was the subject of further clarification being undertaken by Victoria Police and various government departments via the Security and Continuity Networks (SCNs).[243]

The DOJ also provided a list of ongoing projects involving the DPC, the Critical Infrastructure Protection Unit (CIPU) of Victoria Police and the SCN-CG directed at addressing the interpretation issues identified by the Auditor-General:[244]

- in 2010, the CIPU with support from the VMIA commenced a project to develop an electronic tool to identify and rate critical infrastructure. This tool was validated in March/April 2011 within the food sector and has been distributed to other relevant government departments for trial and implementation;
- the SCN-CG has initiated a project to develop a standardised methodology for declaring an essential service;
- under its charter, the CIPU has conducted a number of workshops throughout 2010 and into 2011 with declared essential services and critical infrastructure operators and government department representatives to provided training and development in:
  - national and State protocols and guidelines for Counter Terrorism;
  - exercising standards;
  - Victorian Emergency Management arrangements; and
  - Victoria Police procedures impacting on response and recovery from terrorism events by declared essential services owners/operators.

Findings of the Department of Premier and Cabinet's Review Report

The DPC's *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure* (DPC Review Report) states that there was support amongst stakeholders for the term "essential services" however there was confusion and a lack of understanding about what should be "declared" as an essential service which had resulted in inconsistent treatment between competing operators.[245]

[242] ibid.

[243] Ms P. Armytage, Secretary, Department of Justice, letter to the Committee, received 15 June 2011, p.1

[244] ibid., p.2

[245] Department of Premier and Cabinet, *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure*, 15 June 2011, p.5

In relation to critical infrastructure, the DPC Review Report notes that although the term suggests physical infrastructure rather than encompassing "systems" and "services", the term was supported by government departments and was also consistent with the terminology used in Australian Government policy and by the National Counter-Terrorism Commitee (NCTC) in its *National Guidelines for Protecting Critical Infrastructure from Terrorism.*[246] The Report indicated it was also consistent with the terminology used overseas.[247]

The DPC Review Report proposes that the term "critical infrastructure" be retained but also *"acknowledges that the term is problematic"* for stakeholders. The Report proposes that the revised Framework develop users' understanding of the terminology and explain its relationship to essential services.[248]

Evidence taken at the public hearing

In terms of determining the difference between critical infrastructure and declared essential services, Assistant Commissioner Fontana of Victoria Police advised the Committee that the Victoria Police critical infrastructure database, which includes essential services, comprised approximately 350 sites and that Victoria Police were in the process of using the tool developed with the assistance of the VMIA to review each of the recorded sites to determine whether the site should be classified as critical infrastructure or a declared essential service.[249]

The Committee was advised that this process would take some time to complete due to the size of the database. Assistant Commissioner Fontana advised that the tool had been provided to the relevant departments and the departmental secretaries had been briefed about their responsibilities in respect to critical infrastructure. This briefing was being followed up by a visit to each of the departments to work through their critical infrastructure lists to determine correct classification, redundancy and the identification of any new infrastructure for recording. It is anticipated that once the list has been completely reviewed it will then be reviewed on an annual basis. The Committee was advised that this initial rollout was anticipated to take around 18 months to complete.[250]

At the public hearing, there was a significant amount of discussion about the confusion generated by having two separate administrative arrangements for essential services and critical infrastructure and whether there is a need for some simplification to reduce confusion amongst government departments/agencies and owners/operators of critical infrastructure and to ensure that all infrastructure has been identified and is adequately risk managed and protected.

The Assistant Auditor-General, Financial Audit, Ms Holland, made the following comments at the final session of the hearing:[251]

[246] ibid., pp.6-7

[247] ibid., p.11

[248] ibid.

[249] Mr S. Fontana, Assistant Commissioner, State Emergencies and Securities Department, Victoria Police, transcript of evidence, Session 3, 25 August 2011, p.6

[250] ibid., pp.12-13

[251] Ms E. Holland, Assistant Auditor-General, Financial Audit, Auditor-General's Office, transcript of evidence, Session 5, 25 August 2011, p.5

> *...I think this leads us to a question that we are dealing with as well today and that was asked by the Committee. We got into the fact as to, 'Why can't you have one piece of legislation that covers both declared essential services and critical infrastructure?', and I think that is an interesting question because that would actually get rid of the problem that we noted a number of times today, which is you can talk about essential services and you can talk about critical infrastructure but it is actually the whole cohort. Sure some of them need mandated arrangements around them, but it would be interesting to explore whether then in terms of the framework, the softer option which is about encouragement, why that cannot be encompassed – one framework with encouragement rather than mandate.*

The Chairman of the Committee raised this issue with witnesses throughout the hearing sessions. The Chairman put forward the proposition that Victoria could implement a hierarchical system for critical infrastructure protection management whereby infrastructure and services could be prioritised in terms of their "criticality" with an appropriate scheduling of mandated legislative requirements. In this way there would be one cohort of management supported by an appropriate data recording and reporting system for the collective.[252]

The Chairman invited comment from Assistant Commissioner Fontana of Victoria Police who advised that the issue would require consideration of the amount of regulatory burden on owners/operators of critical infrastructure and essential services and also the amount of work required from Victoria Police and other agencies in supporting that regulatory framework. He stated that under the present arrangements,the operators participating in the SCNs were working well and relationships were continuing to be built.[253]

Representatives from the DPC reiterated that there was a hierarchy of infrastructure already in place with the strongest policy response directed at the risk of a terrorist attack against a "declared essential service". The view is that in the case of declared essential services there are no alternative options, no redundancy, and as such it is considered that legislative and regulatory provisions should apply.[254]

5.2.4 Committee findings and recommendations

The proper identification of critical infrastructure is very important in ensuring that risk management plans are prepared to protect the assets and services from risks or threats and to mitigate the impact of these threats should they eventuate. Where infrastructure is not properly assessed and identified, these assets will be more vulnerable to a variety of risks and threats.

The Committee found that under the current CIP arrangements in Victoria, there is somewhat of a "dual system" in place. Not only is there a need to identify critical infrastructure but there is a further "classification" process required due to the differing arrangements which apply to critical infrastructure and declared essential services (i.e. one set of mandatory requirements

[252] Mr P. Davis MP, Chairman, Public Accounts and Estimates Committee, transcript of evidence, Session 4, 25 August 2011, pp.11-12

[253] Mr S. Fontana, Assistant Commissioner, State Emergencies and Securities Department, Victoria Police, transcript of evidence, Session 4, 25 August 2011, p.12

[254] Mr D. Speagle, deputy Secretary, Federalism, Citizenship and Climate Change, Department of Premier and Cabinet transcript of evidence, Session 4, 25 August 2011, p.12

and one set of voluntary good practice principles). This is discussed further in the following paragraphs.

Classification of critical infrastructure

The Committee acknowledges the work undertaken by the DPC, the SCN-CG and Victoria Police, together with the VMIA, to clarify exactly what constitutes critical infrastructure and what makes critical infrastructure a "declared essential service" for the purposes of the Act. The Committee looks forward to this helping to minimise the inconsistencies and uncertainties in relation to the application of the Act and any future iteration of the CIP policy Framework.

The Committee however wishes to register its concern over the length of time taken to develop a classification process particularly in the light of the original response by the DPC, tabled in the December 2009 Minister for Finance Report, indicating that the project was scheduled for completion by the end of 2009.

The Committee found through evidence given at the hearing that the newly developed tool for applying the new Classification Framework process is in the early stages of being rolled out by Victoria Police and is a sizable task with a rough assessment provided of around 18 months to complete the review of the current critical infrastructure register.[255]

Subsequent advice received from the DPC stated that it is intended that Victoria Police, working with SCN chairs, will complete initial testing of the classification framework for all eight sectors by late 2012.[256] Also the DPC advised that it anticipated that the methodology for identifying declared essential services will be ready for testing by departments in mid to late 2012.[257]

The Committee considers that it would be worthwhile for the DPC and Victoria Police to determine more accurately, the resources to be applied to the task and associated timeframes and target dates for implementation of both the Classification Framework and the methodology to determine declared essential services, which could be approved by the SCN-CG and tracked by that committee on a regular basis. The proposed timelines and updates on progress made should also be reported to the CGRC for noting.

Recommendation 18:

The Committee recommends that the Department of Premier and Cabinet and Victoria Police establish target dates for the implementation of both the *Victorian Infrastructure Classification Framework* and the methodology to determine declared essential services and report this timetable, together with regular progress updates, to the Security and Continuity Network-Coordination Group for approval and monitoring. The project timelines and progress updates should also be provided to the Central Government Response Committee for noting.

[255] Mr S. Fontana, Assistant Commissioner, State Emergencies and Securities Department, Victoria Police, transcript of evidence, Session 4, 25 August 2011, pp.12-13

[256] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 20 October 2011, p.6

[257] ibid., p.7

The need for differing arrangements

The Committee understands the historical context to the promulgation of Part 6 of the Act and notes the explanation provided at the public hearing by the Secretary of the DPC that the former Government's original policy intention was to seek a greater level of assurance through statute that these assets were being appropriately managed against the risk of terrorism.

However, the introduction in 2007 of the CIP policy Framework has led to a dual system of critical infrastructure protection in Victoria which has resulted in some confusion amongst government and industry stakeholders.

In commenting on the existence of both the legislative and CIP policy requirements, the Auditor-General noted in his report:[258]

> *The co-existence of Part 6 of the Act for essential services and the CIP policy Framework for critical infrastructure is complex and challenging for agencies. This co-existence creates confusion and affects coordination between agencies.*

And:[259]

> *It is not clear why there are two sets of arrangements. There is merit in reviewing these arrangements.*
>
> *...since the emergence of national arrangements, subsequent to the 2003 Victorian legislation, it is now timely to review 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 arrangements.*

A read through the recently issued DPC Review Report also reveals how the terms critical infrastructure and essential services continue to be used interchangeably. The Review Report also uses the terms "essential services" and "declared essential services" and acknowledges that guidance notes need to be developed to provide greater detail and direction on how the provisions of the Act and the other more general arrangements are to be applied.[260]

The Committee considers that the management of critical infrastructure and essential services protection in the State is in need of simplification. The existence of legislation for risk management in respect to the threat of a terrorist incident affecting declared essential services and a separate policy encouraging compliance of owners/operators of critical infrastructure represents unnecessary and confusing layers of direction and administration.

The Committee notes the *National Guidelines for Protecting Critical Infrastructure from Terrorism* whose purpose is to provide a consistent approach by the Commonwealth, state and territory governments and business on the protection of critical infrastructure from terrorism.

[258] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.21

[259] ibid., p.24

[260] Department of Premier and Cabinet, *Review of the Arrangements for Managing Risk for Victorian Critical Infrastructure*, 15 June 2011, p.11

The Guidelines state that the Commonwealth has developed the *Critical Infrastructure Protection Risk Management Framework for the Identification and Prioritisation of Critical Infrastructure* to assist the Commonwealth in identifying those assets/facilities which are nationally critical.[261]

The Guidelines nominate five levels of "criticality":[262]

- Vital – alternative sources cannot be provided nationally or by the states/territories. Loss or damage will result in abandonment or long term cessation of the asset;
- Major – severe disruption to facilities/services will result in major restrictions and national assistance will be required;
- Significant – services/facilities will be available but with some restrictions or lower capacity and/or responsiveness. Services may be provided within the state or territory;
- Low – services can be provided within the state or territory or nationally with no loss of functionality; and
- Unknown – insufficient data is available for evaluation.

The Committee asked the DPC whether the *Victorian Critical Infrastructure Classification Framework* makes use of the definitions of criticality referred to in the National Guidelines. The DPC advised:[263]

> *It is Victoria's aim to maximise consistency nationally in the critical infrastructure risk management policy framework. For that reason, the national definitions of critical infrastructure and the criticality levels were adopted in the development of the Victorian Critical Infrastructure Classification Framework.*

Also following on from discussions at the hearing on the need for two systems of administration, the Committee was interested in ascertaining from Victoria Police whether in regard to Victoria's 256 critical infrastructure sites (as reported by the Auditor-General) there were any differences in the degree or level of "criticality" across this cohort which should maybe attract different levels of protection.

The DOJ advised that there were in fact degrees of criticality which are *"weighted in accordance with the risk management framework."* The Department advised that Victoria Police consider all sites important and *"prioritise and focus on those sites that have higher risk ratings."*[264]

In the light of the findings of the DPC Review and information and evidence gathered by the Committee, the Committee is of the view that, in its revision of the current CIP policy Framework, the DPC should consider developing a comprehensive policy which applies to

[261] Attorney-General's Department, National Counter Terrorism Committee, *National Guidelines for Protecting Critical Infrastructure from Terrorism,* 2011, p.3

[262] ibid., p.4

[263] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 20 October 2011, p.7

[264] Ms P. Armytage, Secretary, Department of Justice, letter to the Committee, received 13 October 2011, p.2

both essential services and critical infrastructure and which establishes an integrated approach to the management of all risks, threats and hazards regardless of their source, with compliance requirements based on the level of criticality assigned to the assets or services identified. Specifically the revised policy framework should:

- apply to the total cohort of the State's critical infrastructure;
- include criteria for prioritising or categorising assets and services in terms of their "criticality";
- identify the appropriate risk management regimes and compliance requirements to be applied to different categories of infrastructure by both government agencies and private owners/operators;
- outline an appropriate reporting framework between the owners/operators of critical infrastructure and the relevant departments oversighting their critical infrastructure protection arrangements; and
- include an appropriate system of internal accountability between the relevant departments implementing the policy and the DPC as the agency responsible for strategic leadership of the policy.

Recommendation 19:

The Committee recommends that as part of its revision of the *Victorian Framework for Critical Infrastructure Protection from Terrorism*, the Department of Premier and Cabinet develop a more comprehensive, all encompassing policy framework which specifies relevant and appropriate criteria for determining levels of criticality for the State's critical infrastructure together with specific management regimes applicable to each category and an appropriate reporting framework to improve assurance and accountability over the State's critical infrastructure protection arrangements.

5.3 Risk management

As noted in Chapter Four of this report, today risk management forms an integral component of private and public sector governance arrangements. There is no shortage of literature on the subject and no shortage of mention of risk management principles in both Commonwealth and state public sector policy and legislation. The following paragraphs provide some background information on risk management in the Victorian public sector and its relevance to critical infrastructure protection.

5.3.1 Risk Management Standards

Overarching risk management in both the public and private sector is the international risk management standard ISO 31000:2009 *Risk Management – Principles and guidelines*, which recently replaced the Risk Management Standard AS/NZS 4360:2004. ISO 31000:2009 promotes the implementation of a risk management framework which incorporates an integrated approach to the management of all types of risk.

Also, recently released (June 2010), is AS/NZS 5050:2010 *Business continuity - Managing disruption-related risk*, which explains how to apply ISO 31000:2009 in anticipating disruption-related risks. Emphasis is given in the Standard to disruptive events on a scale beyond the capability of an organisation's normal management system. In particular, the Standard explains how to build contingent capacity into the management framework and prepare contingency plans aimed at stabilising the situation and maintaining or resuming the most critical functions while working towards full restoration of operations. In addition, the Standard refers to pre-event preparations which should include regular maintenance and testing of the contingency plans and contingent capabilities which assist the organisation to respond to an event in an effective manner and transition back to routine management in a planned and controlled way.[265]

5.3.2 Victorian Government Risk Management Framework

As indicated earlier, in March 2011, the Department of Treasury and Finance released the *Victorian Government Risk Management Framework* which updates the previous framework issued in 2007 and takes account of the principles and guidelines set out in ISO 31000:2009. As a minimum, the revised Framework calls for Victorian public sector agencies to risk manage their operations consistent with AS/NZS ISO 31000:2009 (or its successor), the directions issued under the *Financial Management Act 1994* and the *Victorian Government Risk Management Framework*. The Framework states that:[266]

> *A key benefit of the Framework is that it brings together information on governance policies, accountabilities and roles and responsibilities for all those involved in risk management. It also provides a central resource with links to a wide range of risk management information sources.*

The Framework applies to all departments and agencies that report in the annual Financial Report for the State of Victoria but is also recommended to all public sector agencies generally. Specifically, the purpose of the Framework is to provide a minimum common risk management standard for attestation by accountable officers in their annual reports.[267]

The formal attestation in the annual reports states that agencies understand, manage and control key risk exposures consistent with the Standard and that a responsible body or audit committee has verified that view. This is a requirement under the Minister for Finance Standing Directions 4.5.5.[268]

5.3.3 Critical infrastructure risk management

Effective risk management planning is at the crux of effective critical infrastructure protection.

Part 6 of the *Terrorism (Community Protection) Act 2003* mandates the preparation of risk management plans by operators of declared essential services to assess and manage the risk of a terrorist attack. The CIP policy Framework refers to the risk management responsibilities of owners/operators of critical infrastructure under the NCTC critical infrastructure protection guidelines and also to the former Risk Management Standard AS/NZS 4360:2004 against

[265] Standards Australia/Standards New Zealand, *Business continuity – Managing disruption-related risk,* June 2010, pp.2-6

[266] Department of Treasury and Finance, *Victorian Government Risk Management Framework,* March 2011, p.3

[267] ibid., p.6

[268] ibid., p.11

which it states *"all critical infrastructure risk management plans should be assessed."*[269] It is also noted that the CIP policy Framework states that the objectives of critical infrastructure protection include analysing vulnerability and protecting from, and preparing for, all hazards.[270]

Risk management in relation to critical infrastructure is also an integral part of the NCTC's *National Guidelines for Protecting Critical Infrastructure from Terrorism*, and the Commonwealth's *National Strategy for Disaster Resilience* and *Critical Infrastructure Resilience Strategy*.

5.3.4 Other relevant references to risk management and critical infrastructure in Victoria

Emergency management

Part 2 of the *Emergency Management Manual Victoria* is dedicated to "Emergency Risk Management and Mitigation in Victoria". The Manual describes the interconnected relationships between prevention, risk reduction and mitigation.[271]

The Manual also refers to a number of mitigation strategies at a state level such as dangerous goods regulations; food safety regulations; gas and electricity safety codes; immunisation programs; warning systems; community education and awareness programs. It also refers to critical infrastructure protection, noting:[272]

> *Following experiences such as the Longford gas disaster, Victoria has emphasised the importance of protecting the continuity of supply of essential services, particularly within the energy and transport sectors which are privately owned in Victoria.*

Auditor-General's Report: Security of Infrastructure Control Systems

As noted in Chapter One of this report, in October 2010, the Auditor-General tabled an audit report which examined the security of infrastructure control systems (such as Supervisory Control and Data Acquisition (SCADA) systems) at a selection of five water and transport operators and oversight of these operators by the relevant portfolio agencies.[273]

One of the audit findings concerned the development of risk management frameworks and compliance with the requirements of the *Terrorism (Community Protection) Act 2003*. The Auditor-General found that:[274]

[269] Victorian Government, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007, p.10

[270] ibid., p.6

[271] Victorian Government, Office of the Emergency Services Commissioner, *Emergency Risk Management and Mitigation in Victoria — Part 2: Emergency Management Manual Victoria*, February 2005, p.2-2

[272] ibid., pp.2-6, 2-7

[273] Victorian Auditor-General's Office, *Security of Infrastructure Control Systems for Water and Transport*, October 2010, p.vii

[274] ibid., p.15

> *While all operators had developed risk management frameworks and established many of the framework components, none had effective processes to manage the risks to their infrastructure control systems.*
>
> *None of the operators were fully compliant with the risk management requirements of the Terrorism (Community Protection) Act 2003.*

Further the audit raised concerns about a lack of expertise within the relevant portfolio agencies in being able to provide operators with advice about infrastructure control system security and risk, and also business continuity management.[275]

Safety Cases

A safety case regime is an objective-based regime whereby legislation sets broad safety objectives and the operator, who has direct responsibility for the ongoing management of safety, develops the most appropriate methods to achieve the objectives set down. A safety case regime has been used in the nuclear industry in various parts of the world for around 40 years. The methodology was introduced across Europe following a number of chemical incidents and in the offshore petroleum and gas industry in the United Kingdom following an event on a North Sea oil production platform.[276]

The Safety Case sets out the adequacy of the site's safety management system by specifying prevention measures as well as strategies for reducing the effects of a major incident.[277]

The preparation of Gas Safety Cases by operators in the gas industry is a statutory requirement under the *Gas Safety Act 1997* and the *Gas Safety (Safety Case) Regulations 1999*. For example, a Gas Safety Case must include:[278]

- a facility description - which presents an overview of the company's distribution assets and facilities;
- a Formal Safety Assessment (FSA) - which assesses the risks associated with the network including a description of the methodology, identification of hazards, risk assessment and measures taken to reduce risk; and
- a Safety Management System (SMS) - which describes the policies and procedures and control systems in place in relation to managing the safety of the facility and includes reference to: responsibilities; emergency management systems; monitoring; auditing and review; training; and recording and reporting performance.

The Safety Case Summary prepared by Esso for the Longford Crude Oil Stabilisation and Gas Plants states:[279]

[275] ibid., p.23

[276] Government of Western Australia, Department of Consumer and Employment Protection, *MineSafe*, 'The case for safety cases?', volume 14, no.3, September 2005, p.3

[277] WorkSafe Victoria, 'What is a safety case?', <www.worksafe.vic.gov.au/wps/wcm/connect/wsinternet/WorkSafe/Home/Safety+and+Prevention/Your+Industry/Major+Hazard+Facilities/About+the+industry/What+is+a+safety+case/>, accessed 9 August 2011

[278] SP AusNet, *Gas Safety Case — Summary,* February 2007, pp. 3, 6, 8

[279] ESSO Australia Pty Ltd, *Longford Crude Oil Stabilisation and Gas Plants — Safety Case Summary,* 2010, p.12

> *The Safety Case demonstrates how Longford Plants is being managed and operated safely to ensure that risks to personnel are reduced and that potential damage to property, the environment and community is minimised. In particular, the Safety Case illustrates how the major hazards at Longford plants are identified, understood and controlled. It also facilitates further continuous improvement in our safety and reliability performance and provides a mechanism to demonstrate compliance.*

The *Occupational Health and Safety Regulations 2007* also require that all major hazard facilities (i.e. industrial sites handling or processing large quantities of hazardous materials) have a licence to operate, a condition of which is the submission of a Safety Case for approval by WorkSafe Victoria. In Victoria, many major hazard facilities are an essential part of the State's infrastructure. These facilities handle dangerous goods in large quantities and have the potential for major incidents, which can impact on workers, the community and the environment.[280]

To be successful, a safety case regime must have a competent and independent regulator with adequate legal powers. This helps to ensure that the operator prepares the Safety Case in a rigorous manner and those who may be impacted by the facility can have confidence in the judgements of the regulator. The existence of adequate powers of enforcement assist in adding impetus on the operator to ensure the safety case is robust and remedial actions are made where inadequacies in the safety case are highlighted.[281] It has been argued that the development of safety cases has resulted in significant reductions in individual risk, an improved understanding of hazards and risks associated with a facility, enhanced knowledge of the technical and managerial controls required to manage the associated hazards and risks, and better oversight by the regulator.[282]

Energy industry regulation

Under the *Electricity Safety Act 1998* and the *Gas Safety Act 1997*, major electricity companies and all gas companies have a general duty to minimise, as far as practicable, risks to persons and property. These businesses are obliged to submit to Energy Safe Victoria (ESV) for approval, electricity safety management schemes and gas safety cases that set out the safety management systems by which the operators will meet their general safety obligations. ESV assesses these submitted safety management schemes and gas safety cases, audits compliance with them and monitors the companies' safety performance. Electricity generators and other electricity network operators are also under the jurisdiction of ESV and have a statutory duty to operate safely but are not required to submit safety management schemes.[283]

In July 2008, the Energy Networks Association (ENA), which is the peak national body representing Australia's electricity and gas businesses, released a *Proposed National Framework for Electricity Network Safety* as the recommended approach to national

[280] WorkSafe Victoria, *Victoria's streamlined OHS regulation — information sheet*, 'Safety in Victoria's major hazard facilities', June 2007, p.1

[281] P. Wilkinson, National Research Centre for OHS Regulation, Australian National University, *Safety Cases: Success or Failure?*, May 2002, p.6

[282] K. Heiler, National Research Centre for OHS Regulation, Australian National University, *Is the Australian Mining Industry Ready for a Safety Case Regime?*, March 2006, pp.8-9

[283] Australian Energy Regulator and Energy Safe Victoria, *Memorandum of Understanding*, December 2009, p.4

electricity network safety regulation. The Proposed Framework sets out the scope for a safety case for electricity businesses which manage networks characterised by extensive distribution throughout the public domain such as powerlines, substations and underground cables. The safety case, approved by a relevant regulator would also provide the basis for compliance with Occupational Health and Safety (OHS) legislation and regulation. The ENA believes a national approach is supported by the economic regulation by the Australian Energy Regulator and moves in OHS regulation towards national alignment.[284]

5.4 Auditor-General's review of the audit and validation of critical infrastructure risk management plans

Section 32 of the *Terrorism (Community Protection) Act 2003* requires the operator of a declared essential service to ensure that the risk management plan (developed for that declared essential service under Section 29 of the Act) is audited annually to ensure it adequately meets the requirements of Section 31, which outlines what a risk management plan must contain for the purposes of the Act.[285]

Under the CIP policy Framework, the specific responsibilities of Victoria Police include assisting owners/operators of critical infrastructure in their development, validation and audit of risk management plans.[286]

5.4.1 Auditor-General's findings and recommendation

The Auditor-General reviewed the activities of three departments with declared essential services in their sector and found at the time of the audit that:[287]

- in the water sector, declared essential services were in the first year of their compliance cycle and so no audits had been undertaken. The responsible department was intending to work with water industry operators to develop guidance for the annual audit;
- in the energy sector, the responsible department had engaged a private provider to review a sample of risk management plans to assess compliance with the Act and to make suggestions for improvement; and
- in another department, some of the files containing records from owners/operators in relation to their risk management plans, audit certificates and training activities were incomplete.

In relation to the preparation of risk management plans by owners/operators of critical infrastructure, Victoria Police advised the Auditor-General that information was not available to determine how many risk management plans had been validated or audited.[288]

[284] Energy Networks Association, 'Peak Energy Body Proposes National Framework for Electricity Safety', 15 July 2008, <http://www.ena.asn.au/?p=752> accessed 9 August 2011

[285] *Terrorism (Community Protection) Act 2003*, s. 32

[286] Victorian Government, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007, p.18

[287] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.52

[288] ibid., p.53

The Auditor-General also found that there was no definition or guidelines in place to assist interpretation of the term "audit" or "auditor" under the Act or for the purposes of the CIP policy Framework.[289]

The Auditor-General recommended that the DPC provide clear guidance on terminology used, such as "audit", "auditor" and "adequacy of the exercise", to assist departments, Victoria Police and operators of declared essential services to implement requirements more reliably (Recommendation 5.2).[290]

5.4.2 Response by the Department of Premier and Cabinet

The response of the Department as detailed in the Minister for Finance Report states that the best method for ensuring guidance on terminology and definitions is being considered as part of the review of the CIP arrangements including Part 6 of the legislation.[291]

5.4.3 Subsequent developments noted by the Committee

The Department of Premier and Cabinet's Review Report

The DPC Review Report revealed that there was some concern amongst stakeholders about the lack of definition and prescription in the Act in relation to the quality of risk management plans, the extent of the audit required of those plans and who should undertake those audits.[292]

In another section of the DPC Review Report which discusses the implementation by departments of arrangements required under the Act, the DPC states that the limited guidance available to government departments has resulted in inconsistency and inability to benchmark for best practice, particularly in areas of exercising and auditing.[293]

In a section headed "leadership and governance", the DPC Review Report states: [294]

> *There is no "best practice" model for the overall governance of the arrangements. However, a good governance structure would provide standardised auditing templates, a validation process for adequacy of exercises, and the ability to share lessons learnt from implementing the arrangements. Information on exercise compliance and feedback can be provided through formal guidance developed by departments.*

The solution as posed in the DPC Review Report is for Victoria Police to establish a working group of representatives from government departments and industry to develop guidance notes explaining the requirements of Part 6 of the Act.[295]

[289] ibid.

[290] ibid., p.59

[291] Department of Treasury and Finance, *Response by the Minister for Finance to the Auditor-General's Reports issued during 2008-09,* December 2009, p.106

[292] Department of Premier and Cabinet, *Review of the Arrangements for Managing Critical Infrastructure,* 15 June 2011, p.6

[293] ibid., p.13

[294] ibid., p.14

[295] ibid.

Review of CIP risk management plans by Victoria Police

As stated Victoria Police have a clear role to play under Part 6 of the Act in relation to supervising exercises to test the adequacy of risk management plans of declared essential service operators in regard to the threat of a terrorist incident.

Correspondence received by the Committee from the DOJ in June 2011 advised that to date the definition of "adequacy" as it refers to training exercises conducted by owners/operators of declared essential services remains unclear. Victoria Police advised that it is developing an appropriate definition for consideration and ratification by the SCN-CG.[296]

Evidence taken at the hearing suggested that the supervision of risk management training exercises of declared essential service operators under Part 6 of the Act had been diligently performed by Victoria Police.

Under the CIP policy Framework, Victoria Police are required to *"assist owners/operators of critical infrastructure in their development, validation and audit of risk management plans."*[297] Following the hearing, the Committee sought additional clarification from Victoria Police of the extent of their involvement with the risk management and business continuity plans of critical infrastructure operators.

The DOJ responded:[298]

> *Critical infrastructure is not declared and there is no legislation that addresses the issue of its business continuity plans and risk management plans. Police members provide advice or assess the appropriateness of these plans in regard to emergency response arrangements as part of the risk management and business continuity plan in the event of a threat or incident…CIPU members undertake a physical site assessment of Critical Infrastructure premises and make recommendations only in respect to the security and vulnerability of those sites, when invited by the owner/operator.*

The DOJ advised the Committee of an industry-emergency response agency network in Central Gippsland which provides an example of "best practice" in the area of the development of risk management and business continuity plans. The Central Gippsland Essential Industries Group (CGEIG) involves operators of both critical infrastructure and declared essential services together with the local emergency response agencies to test their respective emergency preparedness.[299]

Shared responsibility for risk management and risk transfer

Discussion of critical infrastructure risk management issues during the public hearing with representatives from the DPC focussed on the identification and management of interdependent risks in industry sectors and on the issue of "risk transfer" from the owners/operators of critical infrastructure to the government.

[296] Ms P. Armytage, Secretary, Department of Justice, letter to the Committee, received 15 June 2011, p.3

[297] Victorian Government, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007, p.18

[298] Ms P. Armytage, Secretary, Department of Justice, letter to the Committee, received 13 October 2011, p.1

[299] ibid.

The Secretary, DPC stressed to the Committee that while the Government recognised it had a responsibility to ensure the continuity of essential services, it has limited control over the assets and services, hence the risk management requirements under Part 6 of the Act directed at what was seen to be greatest risk at the time i.e. terrorism.[300] The Secretary also stated that it was important to note when considering the best approach, *"that we recognise that we do not want to have risk transfer to the State in these arrangements.*"[301]

Following the hearing, the Committee requested further elaboration from the DPC on government responsibility for CIP and the issue of "risk transfer". The DPC advised:[302]

> *The Act and accompanying regulations reflect international best practice in that they recognise different levels of responsibility, but are explicit in explaining that owners and operators of declared essential services, who are best placed through their intimate knowledge of their systems and facilities, must determine risks and mitigation strategies.*
>
> *…*
>
> *…Government's role is to assist. If a more prescriptive role was taken by Government, the private sector could use this as an opportunity to transfer risk to Government.*
>
> *…*
>
> *Nevertheless, in recognition of the importance of the continuing supply of essential services provided by these assets to the Victorian community, government has developed through its arrangements a cooperative partnership with the asset owners and/or operators. This approach provides assurance to the community that Government recognises the importance of these assets and is taking measures to provide for continuity of the services they provide.*

There was further discussion at the hearing about whether the "all hazards" approach to managing risks should be mandated in the legislation and the shift at the national policy level to adopt the concept of "critical infrastructure resilience" which also requires "shared responsibility" in relation to preparing for, and responding to, risks. Mr Mark Duckworth, Executive Director Citizenship and Resilience, DPC, made the following comment in relation to the role of government in this area of public policy:[303]

> *I think we should be very careful about going down a path that in fact undermines the resilience of organisations and companies so that they believe that in fact they do not have to maintain their responsibilities, which as a matter of good corporate governance they should do. It has been articulated in an number of reports and indeed quoted in the Auditor-General's report that as a matter of good governance companies should look after their own assets…The issue is that if the policy of the United States, the policy of the UK and the policy of every other jurisdiction in Australia is based upon that method* [i.e. a collaborative or guidance role for government]*, why is it we*

[300] Ms H. Silver, Secretary, Department of Premier and Cabinet, transcript of evidence, Session 2, 25 August 2011, p.3

[301] ibid., p.4

[302] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 20 October 2011, p. 4

[303] Mr M. Duckworth, Executive Director, Citizenship and Resilience, Department of Premier and Cabinet, transcript of evidence, Session 4, 25 August 2011, p.13

> *should move down a different path in Victoria? What are the implications for that? I think it is just an issue that is worth the Committee considering.*

5.4.4 Committee findings and recommendations

In reviewing critical infrastructure risk management arrangements, the Committee found that there are a number of issues which require reflection in the future. These are:

- definition and interpretation of the risk management requirements set out in the legislation and the CIP policy Framework;
- risk management responsibilities of Victoria Police and relevant departments under the CIP policy Framework;
- critical infrastructure risk management for all hazards; and
- risk management compliance by owners/operators and the need for mandatory terrorism risk management requirements.

The Committee's findings in relation to each of these issues are presented in the following Sections.

5.4.5 Definition and interpretation of critical infrastructure protection risk management requirements

It is now eight years since the Act came into operation and fours years since the CIP policy Framework was released. The Committee is concerned about the length of time taken for the DPC to initiate steps to clarify the definitions and terminology used in the policy and legislation to assist Victoria Police, the relevant government departments and the owners/operators of critical infrastructure and declared essential services with interpreting the requirements of the legislation and the policy to promote consistent and appropriate compliance.

The Committee considers that the DPC needs to ensure that concepts and definitions in relation to the preparation of risk management plans and the testing of those plans are clearly and consistently defined in any revised CIP policy Framework to limit any confusion and assist in ensuring obligations are consistently understood and satisfactorily met.

In the interim, the Committee considers that there is a pressing need for the development of clear guidelines for both Victoria Police and operators of essential services in regard to their risk management obligations under the legislation. Further clarification is also needed in relation to the risk management and audit principles referred to in the CIP policy Framework.

The Committee notes the establishment of a working group led by Victoria Police to develop guidance notes to establish a common understanding of the requirements of Part 6 of the Act. However, the Committee considers there is also a need for the DPC to clarify the policy obligations of departments/agencies under the current CIP policy Framework in respect to the risk management of critical infrastructure within their portfolios.

Recommendation 20:

The Committee recommends that the Department of Premier and Cabinet ensure that any revised critical infrastructure protection policy for the State includes clearly defined and agreed terminology in relation to the preparation, audit and testing of risk management plans to limit confusion and inconsistency and to assist stakeholders in the effective application of the *Terrorism (Community Protection) Act 2003* and associated policy.

5.4.6 Critical infrastructure risk management obligations of Victoria Police and relevant departments/agencies

With regard to risk management concepts and principles contained in the CIP policy Framework, the Committee considers that there is a need for the relevant departments together with Victoria Police to actively encourage owners/operators of critical infrastructure in their sectors to develop risk management plans and to ensure that these plans are regularly tested and audited.

The Committee notes that the CIP policy Framework specifies the following risk management related policy obligations of lead departments in the protection of the State's critical infrastructure and essential services:[304]

- for the DOT – Ensure there is adequate management of security risks and emergencies within portfolio-led critical infrastructure sectors: public transport, road and rail system, ports and marine environment, and freight;

- for the DSE – Ensure water authority compliance with policy and regulatory requirements, particularly in the area of emergency management and protection of critical infrastructure;

- for the DPI (Energy Division) – Ensure there is adequate management of security risks and emergencies within the portfolio-led critical infrastructure energy industries sector; and

- for the Department of Business and Innovation (DBI) (financial services portfolio and Multimedia Victoria) – contribute to adequate management of security risks and emergencies within the Banking and Finance sector and the Information and Communications Technologies sector.

It is imperative that departments have adequate processes in place to check that owners/operators of both critical infrastructure and essential services are aware of their responsibilities to undertaken comprehensive planning to ensure that all risks and hazards have been identified and strategies have been developed to prepare the organisation for the possible occurrence of security risks and/or threats. Comprehensive risk management planning should encompass adequate processes to test the validity of risk management, crisis management and continuity planning arrangements.

[304] Victorian Government, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007, pp.19-22

Recommendation 21:

The Committee recommends that all departments/agencies with key roles and responsibilities in relation to the support of critical infrastructure protection have appropriate processes and systems in place to ensure they are meeting their obligations under both Part 6 of the *Terrorism (Community Protection) Act 2003* and the current *Victorian Framework for Critical Infrastructure Protection from Terrorism*.

Recommendation 22:

The Committee recommends that the Security and Continuity Network-Coordination Group review the critical infrastructure risk management monitoring and reporting arrangements established by relevant departments in an effort to identify examples of best practice which can be used to assist improvement in other departments/agencies.

5.4.7 Critical infrastructure risk management for all hazards

Public policy and legislation must be responsive to changes and developments in the operating environment in order to remain relevant and effective. As already stated, the focus of the mandated requirements in Part 6 of the Act is the risk of a terrorist incident.

The Committee notes the shift in emphasis in relation to disaster management preparedness and response and critical infrastructure protection at the national level, which has been adopted by COAG. The Committee also notes incidents which have been caused by risks and threats other than a terrorist attack. In the example of the Longford Gas explosion, disruption to supply was as a result of an operational problem and not a terrorist incident. In the example of the Maroochy Shire, sewage spills were the result of industrial sabotage by a disgruntled ex-contractor. In a recent report, the US military network operating the air force drone fleet has been reportedly infiltrated by a computer virus.[305] These examples demonstrate the importance of vigilance, awareness and appropriate preparedness against a range of risks/threats. As such, the Committee is of the view that critical infrastructure risk management should consider a comprehensive range of risks and threats and not just the risk of a terrorist incident.

The Committee acknowledges that the DPC Review Report recommends that a revised CIP policy Framework "*explicitly address risks on an all hazards approach*"[306] and considers this an important development given the threats and risks which have manifested in Australia and internationally in recent times. The Committee notes also the DPC recommendation in the Review Report that no amendments be made to the Act.[307]

The Committee considers that, in the interim, departments/agencies with responsibilities for supporting critical infrastructure protection take a proactive approach in promoting the, COAG agreed focus of building resilience and the "all hazards" approach in their oversight

[305] ABC News, *Virus strikes US drone fleet,* 9 October 2011, <www.abc.net.au/news/2011-10-09/computer-virus-hits-us-drone-fleet/3403024>, accessed 10 October 2011

[306] Department of Premier and Cabinet, *Review of the Arrangements for Managing Critical Infrastructure,* 15 June 2011, p.10

[307] ibid., p.9

of risk management by all owners/operators of critical infrastructure and essential services within their portfolios.

Recommendation 23:

The Committee recommends that relevant departments/agencies with key roles and responsibilities in relation to the support of critical infrastructure protection implement actions to promote and encourage an all hazards approach to risk management by owners/ operators of critical infrastructure and essential services within their portfolios to ensure that strategies have been developed to prepare for the possible occurrence of a range of security risks and threats.

5.4.8 Risk management compliance by critical infrastructure owners/ operators

Based on the Auditor-General's findings and information received by the Committee, it appears that, currently, there is no way of comprehensively assessing the level of satisfactory compliance by industry owners/operators of critical infrastructure and essential services with the risk management provisions outlined in the Government's CIP policy. However, some information is available through Victoria Police of compliance by declared essential services operators with the terrorist risk management training exercises under Part 6 of the Act.

The Committee has noted already the responses of the DPC and Victoria Police that the most critical infrastructure warrants mandated risk management requirements. The Committee also notes that while the DPC Review Report recommends an "all hazards" approach to risk management under a revised CIP policy Framework it also recommends that no amendments to the mandated provisions of the Act be made at this time. A review of the legislation is scheduled by 30 June 2013.

As noted in this report there are a whole suite of standards, legislation and regulations outlining risk management requirements and providing good guidance on risk management principles for both the private and public sectors. Namely:

- ISO 31000:2009 and AS/NZS 5050:2010;
- the *Victorian Government Risk Management Framework*;
- the *Emergency Management Manual Victoria*;
- national disaster resilience and critical infrastructure resilience strategies;
- the *National Guidelines for Protecting Critical Infrastructure from Terrorism* and the National Counter Terrorism Committee which organises regular and comprehensive training exercises to test preparedness and emergency response; and
- statutory safety requirements under the *Electricity Safety Act 1998* and the *Gas Safety Act 1997* and also under the *Occupational Health and Safety Regulations 2007.*

Some of these examples indicate that the regulatory burden on the energy industries is already significant.

The Committee considers that these overlapping strategies and regulations need to be taken into account as part of the forthcoming review of the *Terrorism (Community Protection) Act 2003* and in particular in regard to whether the mandatory risk management provisions outlined in Part 6 of the Act are adding value or whether there is a more efficient way of proceeding.

Existing industry legislation, regulations and contract/licensing arrangements between the State of Victoria and the owner/operator, also provide a range of options which could be explored as a method of obtaining some level of assurance by way of certification or declaration by the owners/operators of critical infrastructure and essential services that adequate risk management plans have been prepared in accordance with ISO 31000:2009 and/or other national or state policy.

Recommendation 24:

The Committee recommends that the Department of Premier and Cabinet investigate avenues available through existing industry legislation, regulations or contract/licensing agreements for industry owners/operators to provide some certification or assurance that they, the owners/operators of critical infrastructure and essential services, are taking appropriate action to protect Victoria's critical infrastructure and essential services from a range of identified risks and hazards.

5.5 Training exercises and continuous improvement

Section 33 of the Act requires the operator of a declared essential service to prepare and participate in a training exercise at least once each year to test the operation of their risk management plan. The section also requires that the training exercise must be conducted at a time and place determined by the responsible Minister in consultation with the operator and the Chief Commissioner of Police and must be supervised by the Chief Commissioner of Police.[308]

As noted, tnder the CIP policy Framework, Victoria Police is required to assist owners/operators of critical infrastructure in the development, validation and audit of their risk management plans.[309] Also, relevant departments have certain responsibilities in relation to risk and emergency management within their industry sectors.

5.5.1 Auditor-General's findings and recommendation

The Auditor-General reviewed the activities of relevant departments and Victoria Police in performing their risk management and training oversight responsibilities in relation to both Part 6 of the Act and the CIP policy Framework.

[308] *Terrorism (Community Protection) Act 2003*, s. 33

[309] Victorian Government, *Victorian Framework for Critical Infrastructure Protection from Terrorism*, April 2007, p.18

The Auditor-General found that both the DPI and the DOT had conducted regular training activities as required under Part 6 of the Act. The DSE and four operators of essential services in the water sector had also conducted exercises to test their risk management plans.[310]

The Auditor-General found that the other departments with responsibilities for critical infrastructure protection within their industry sectors had played no active role in testing risk management plans in their sectors under either the legislation or the CIP policy Framework. The Auditor-General did note, however, that all six departments had been involved in training exercises to test their emergency management response under either Victoria's broader emergency management arrangements or as part of national exercises.[311]

With regard to monitoring risk management planning by critical infrastructure owners/ operators, Victoria Police advised the Auditor-General that it does not have the available resources to ensure that all risk management plans for critical infrastructure are tested annually but that it does attend training exercises of which it is notified.[312]

Reporting on training exercises

In noting that departmental emergency management training exercises take place periodically, the Auditor-General reviewed a number of reports on the results of these training exercises to assess their effectiveness and the extent to which findings have driven improvement.

The Auditor-General found that, Victoria Police maintain a "lessons learned" database in which it records the outcomes of NCTC coordinated exercises and, agencies retain the results of their training exercises separately within their own departmental files. The report concluded that the lack of a central repository for retaining the results of all emergency training exercises made collective analysis of the outcomes difficult.[313]

The Auditor-General recommended that:[314]

- the DPC and Victoria Police consult with departments and seek to standardise reporting on training exercises conducted under both Part 6 of the Act and in accordance with the CIP policy Framework to enable lessons learned to be more easily identified and future training exercises to be improved (Recommendation 5.3); and
- the reports on the results of training exercises should be stored centrally to facilitate comprehensive analysis of the outcomes across exercises (Recommendation 5.4).

[310] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, pp.53-4

[311] ibid., pp.54-5

[312] ibid., p.54

[313] ibid., p.57

[314] ibid., p.59

5.5.2 Response by the Department of Premier and Cabinet and the Department of Justice

The response of the DPC as detailed in the Minister for Finance Report refers to the establishment in 2006 of a centralised exercise management group within the Office of the Emergency Services Commissioner (OESC) to coordinate counter terrorism and emergency management exercises. The DPC also stated that this role includes maintaining a record of the outcomes of the exercises to facilitate continuous improvement. The Department stated that it had worked with Victoria Police and the OESC to revise the structures and oversight of all multi-agency training exercises and that a State Exercise Steering Committee has been established.[315]

Further in relation to the maintenance of the results of training exercises in a secured central repository, the DPC stated that it has developed guidance on standards for securing security classified information.[316]

The response of the DOJ as detailed in the Minister for Finance Report provided no details as to actions proposed to address the recommendations except to say they were supported.[317]

5.5.3 Subsequent developments noted by the Committee

Department of Premier and Cabinet

The Committee wrote to the DPC in May 2011 asking for an update on the operation of the State Exercise Steering Committee in terms of its membership, functions and recent activities. In addition, the Committee asked the DPC to comment on how the actions taken have improved Victorian emergency management arrangements.

The DPC advised that the State Exercise Steering Committee (within the OESC) is a sub-committee of the State Multi-Agency Emergency Management Training and Exercising Strategy Committee (EMTESC), also within the OESC, and its purpose (as set out in the Emergency Management Manual Victoria) is:[318]

> *…to develop a multi-agency emergency management exercise strategy and oversee the implementation of development exercise programs in line with strategic operational direction provided by EMTESC.*

The DPC further advised that the State Exercise Steering Committee meets on a monthly basis and is chaired by a senior officer of the OESC. Its members comprise representatives from:[319]

- Ambulance Victoria;
- the Country Fire Authority;

[315] Department of Treasury and Finance, *Response by the Minister for Finance to the Auditor-General's Reports issued during 2008-09,* December 2009, p.106

[316] ibid.

[317] ibid., p.64

[318] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.12

[319] ibid., pp.12-13

- the Metropolitan Fire Authority;
- Department of Human Services;
- Department of Premier and Cabinet;
- Department of Sustainability and Environment;
- Department of Transport;
- Victoria Police; and
- the Victoria State Emergency Service.

The State Exercise Steering Committee has an "all-hazards, all agency" approach to emergency management exercises and where appropriate, the relationship between counter-terrorism and emergency management is included as part of general exercising and training.

However, the DPC advised that while counter-terrorism exercises are included in the broad spectrum of the State emergency training exercise regime, the State Exercise Steering Committee does not have a mandate to oversee counter-terrorism training exercises under Part 6 of the Act. Further, the Department advised that the OESC is not provided with an exercise debriefing for any of the training conducted required under Part 6 of the Act. This Part involves only the operator of the essential service, the relevant department and Victoria Police.[320]

Department of Justice

The Committee wrote to the DOJ in May 2011 asking for specific details about actions taken to address the issues raised by the Auditor-General in relation to standardising the reports on training exercises and ensuring reports are stored centrally to allow for the results to be consolidated.

The DOJ advised the following:[321]

- Victoria Police monitors the lessons learned from its assessment of training exercises to assist continuous improvement in the area. The sharing of knowledge and awareness of critical infrastructure and declared essential services issues between various government departments has been the subject of an ongoing program;
- exercise feedback reporting, compliance letters and debriefs undertaken by Victoria Police as part of their responsibilities in assessing training exercises under Part 6 of the Act have now all been standardised; and
- the CIPU of Victoria Police retains centralised hard copy files on all declared essential services owner/operators containing information relating to their Part 6 annual training exercise. The industry operators and relevant departments also retain this information as part of their responsibility for undertaking training exercises under Part 6 of the Act.

[320] ibid., p.13

[321] Ms P. Armytage, Secretary, Department of Justice, letter to the Committee, received 15 June 2011, pp.3-4

The DOJ also advised that funding has been requested from the NCTC for an exercise program aimed at enhancing cooperation between sectors and jurisdictions. The workshops and exercises under the proposed program will be aimed at government agencies and critical infrastructure owners/operators.[322]

5.5.4 Evidence taken at the public hearing

Supervision of exercises by Victoria Police

At the public hearing representatives of Victoria Police gave evidence to the Committee of the extent of work undertaken in monitoring the risk management plans of critical infrastructure owners/operators and the testing of those plans.

The then Acting Chief Commissioner of Police, Mr Ken Lay, advised that the CIPU had conducted 36 visits to critical infrastructure and declared essential services sites during the 2010-11 financial year. These visits had included an update of the relevant operators contact details and a security risk assessment of the site. Reports of each assessment were provided to the operator and to regional emergency management members.[323]

The then Acting Chief Commissioner advised the Committee that there is no legislative requirement for critical infrastructure operators to exercise on a regular basis.[324] Where requested, Victoria Police participate in any emergency training exercises conducted by the owners/operators of critical infrastructure sites and participate in the Part 6 exercises of declared essential service operators. Victoria Police encourage critical infrastructure owners/operators to consider recommendations made in relation to their risk management plans to achieve appropriate outcomes however they are under no compulsion to comply.[325]

With regard specifically to Part 6 exercises, Assistant Commissioner, Mr Stephen Fontana, advised that Victoria Police oversight 39 exercises each year and have only had one occasion where an operator has failed a test. Victoria Police provide advice to operators and incorporate lessons learned from an exercise into the next exercise that is conducted in an effort to improve plans. There is an expectation that those operators will work with the relevant department to build their capability where gaps are identified.[326]

With regard to training exercises under Part 6 of the Act, the then Acting Chief Commissioner of Police advised that declared essential service operators are encouraged to share feedback from CIPU reports with their relevant government department as a way of contributing to continuous improvement in their security risk management plans and emergency planning, response and recovery. There is no compulsion for this information to be shared, nor are there any statutory provisions that recommendations be acted upon by declared essential service operators.[327]

[322] ibid., p.4

[323] Mr K. Lay, Acting Chief Commissioner, Victoria Police, transcript of evidence, Session 3, 25 August 2011, p.3

[324] ibid., p.7

[325] ibid., p.3

[326] Mr S. Fontana, Assistant Commissioner, State Emergencies and Securities Department, Victoria Police, transcript of evidence, Session 3, 25 August 2011, p.4

[327] Mr K. Lay, Acting Chief Commissioner, Victoria Police, transcript of evidence, Session 3, 25 August 2011, p.7

Emergency management training and preparedness to respond – Emergency services

The Secretary of the Department of Justice advised that the Department has no legislated responsibilities under the *Terrorism (Community Protection) Act 2003* but have a role to play through the CIP policy Framework in their involvement in the Police and Emergency Services SCN which is co-chaired by Victoria Police and the OESC. Under the *Emergency Management Act 1986* the Department has very significant responsibilities in terms of ensuring that *"there is appropriate testing and exercising and management of a range of all-hazard emergency management matters across the State."*[328]

Extensive discussion took place at the hearing with representatives from the Department of Justice about emergency management arrangements in the State. The recent natural disasters, the findings of the 2009 Victorian Bushfires Royal Commission and the current inquiry into the Victorian floods response indicate that there has been, and continues to be, a significant amount of attention on emergency management response in the State.

The Secretary, DOJ, Ms Armytage also directed the attention of the Committee to the recent release of the Victorian Government's Green Paper on emergency management which seeks to address criticisms raised in the Victorian Bushfires Royal Commission concerning organisational arrangements and the "silo" approach across the public sector. The review will also consider the large amount of emergency legislation and will seek to clarify the emergency management framework in place in the State.[329]

Ms Armytage stated that an extensive amount of work has been undertaken through the Victorian Emergency Management Council in the last few years to ensure appropriate multi-agency training is occurring and regularly reported on in terms of improvement. Since 2009 there has been substantial investment by the State Government in emergency management largely as a result of the 2009 bushfires and more recently floods in the State. Ms Armytage stated that:[330]

> *Whilst that has not been directly attributed to counter-terrorism, we think much of the infrastructure enhancements and capability enhancements that are demonstrated through that investment will ultimately benefit the emergency sector, should it be required to respond to a terrorism event in the future.*

At the public hearing, the Committee also heard evidence from representatives of Victoria Police and the OESC about the range of training activities conducted in the State involving emergency services agencies and departments. The Committee was advised that Part 6 exercises are clearly the mandated responsibility of Victoria Police. However, the Acting Emergency Services Commissioner advised that there is a very close relationship with the OESC because:[331]

> *...the consequences of a terrorist incident, the response to an explosion in an emergency management context, is the same despite whether it is a bomb*

[328] Ms P. Armytage, Secretary, Department of Justice, transcript of evidence, Session 3, 25 August 2011, p.4

[329] ibid., pp.9-10

[330] ibid., p.5

[331] Mr J. Buffone, Acting Emergency Services Commissioner, Office of the Emergency Services Commissioner, transcript of evidence, Session 3, 25 August 2011, p.10

> *or a gas explosion or anything else. It is about about aligning those two and making sure that there is that genuine all-hazards and joined-up approach.*

In terms of de-briefing other emergency services organisations, such as the OESC, in relation to exercises under Part 6 of the Act, the Committee was advised that because of the security sensitive nature of the information, this information was retained exclusively by Victoria Police. The Acting Emergency Services Commissioner was asked whether this should be re-considered in the light of the increasing emphasis on preparing for natural disasters and also "all hazards" in relation to critical infrastructure protection.

The Acting Emergency Services Commissioner advised the Committee that whilst the details from these exercises are not circulated in a formal sense, emergency services organisations and relevant departments are involved with Victoria Police on a number of committees and networks which share information about training and preparedness in the development of strategies and programs which are implemented in an "all hazards" environment.[332]

The Acting Emergency Services Commissioner agreed that there were instances where information could not be openly shared because it would represent a security risk. However, there were improvements which could be made to the way lessons learned could be exchanged and some action has been taken in recent times to facilitate that.[333]

The Secretary, DOJ stressed to the Committee that much of the security-related information relates to details of prevention and risk mitigation whereas, once an event has occurred then the consequent management is about how to respond. The Secretary stated:[334]

> *I think the distinction there is really that there cannot be sharing of all information about what hazards or risks are being planned for – the secure information. Once the event has occurred, we do have to have this very open and transparent way that our normal emergency management events kick in and benefit from all those other exercises that have been done in case there was a natural hazard, a major accident or something of that case.*

The Committee noted that within the OESC are a range of emergency training and exercise management groups and committee with the following roles:

- the Emergency Management Exercise Group's goal is to provide a standardised approach to exercise planning and coordination, with a focus on outcomes that enable organisations and emergency service agencies to enhance capability and interoperability;[335]

[332] ibid., p.11

[333] ibid., p.12

[334] Ms P. Armytage, Secretary, Department of Justice, transcript of evidence, Session 3, 25 August 2011, p.12

[335] Office of the Emergency Services Commissioner, *Emergency Management Exercise Group,* <www.oesc.vic.gov.au/home/training+and+exercising/oesc+-+emergency+management+exercise+group>, accessed 29 April 2011

- the Multi-Agency Emergency Management and Exercising Strategy Committee has a mandate under the *Emergency Management Act 1986* to provide strategic direction for the identification, planning and conduct of emergency management training and exercising for emergency service organisations in Victoria;[336] and

- the State Exercisie Steering Committee which is a sub-committee of the Multi-Agency Emergency Management and Exercising Strategy Committee, has a role to develop a multi-agency emergency management exercise strategy and implement program, resources and competencies in line with strategic operational direction.[337]

Given its extensive role in emergency management training, following the hearing, the Committee was interested in seeking the views of the DOJ in relation to the possibility of greater involvement from the OESC, through the State Exercising Committee in conducting training exercises directed at testing the emergency preparedness of owners/operators of critical infrastructure and essential services to a range of risks and hazards and not exclusively terrorism.

The DOJ advised the Committee that with the OESC moving towards a regulator and inspectorate model, it would be appropriate for the agency to have a role testing the emergency preparedness of owners/operators. Such a role would not be envisaged to replace the existing regime of relevant departmental responsibilities but *"could be an independent assessor of preparedness, which could assist in driving quality, accountability and improvement."*[338]

5.5.5 Committee findings and recommendations

The conduct of adequate and relevant emergency training preparedness is obviously of significant importance to emergency services agencies in the public sector and also to a number of government departments because in the event of an emergency incident of any nature, it is government agencies, community and volunteer organisations which are in the front line of response. Private sector businesses, including those responsible for managing the State's critical infrastructure and essential services, also have serious responsibilities in terms of being as well prepared as possible for an emergency incident impacting on the assets and/or infrastructure under their control.

The Auditor-General did not include any review of the State's emergency management arrangements as part of his audit review. The Auditor-General's review focussed on "preparedness to respond" not the response after an incident. Also the focus of the audit was on a preparedness to respond to a terrorist incident and not preparedness for "all hazards".

It is reasonable to note that there is a significant amount of overlap between arrangements in place for emergency response preparedness and emergency response arrangements.

[336] Office of the Emergency Services Commissioner, *Multi-Agency Emergency Management Training and Exercising Strategy Committee,* <www.oesc.vic.gov.au/home/training+and+exercising/oesc+-+multi-agency+emergency+management+training+and+exercising+strategy+committee>, accessed 2 June 2011

[337] Office of the Emergency Services Commissioner, *State Exercise Steering Committee,* <www.oesc.vic.gov.au/home/training+and+exercising/oesc+-+state+exercise+steering+committee>, accessed 2 June 2011

[338] Ms P. Armytage, Secretary, Department of Justice, letter to the Committee, received 13 October 2011, p.2

Evidence provided to the Committee by representatives from the DOJ, Victoria Police and the OESC suggested that a significant amount of effort is put into the planning and conduct of emergency management preparedness training for a range of threats and hazards, including the threat of a terrorist incident.

As stated earlier, in terms of testing the level of preparedness of operators of declared essential services to a terrorist incident, the Committee was of the view that Victoria Police has sought to perform its responsibilities under Part 6 of the Act diligently and professionally.

However, the Committee found that the level of preparedness in relation to the operators of critical infrastructure sites not covered by the provisions of Part 6, is less easy to assess as the information appears to be spread across a number of relevant departments who, according to the Auditor-General, have systems and procedures of varying quality in place to monitor and oversee the risk management plans and emergency preparedness of these operators.

The Committee is concerned that whilst there are exercises being undertaken and information and knowledge generated within a number of agencies as a result, there does not appear to be a systemic process whereby this information is passed to a central repository to make further use of the information.

The Committee notes that the OESC has significant responsibilities in relation to emergency management training and exercising. The Committee has noted that in October 2010, a *State Emergency Management Training and Exercise Strategic Framework* was developed under the direction of the State Multi-Agency Emergency Management Training Committee within the OESC. This Framework aims to:[339]

- provide a rolling three year multi-agency training and exercising program that identifies areas of common purpose and seeks to facilitate joint training;
- ensure the emergency management multi-agency training and exercising is all hazards focussed and includes planning, response and recovery;
- implement a multi-agency training and exercising program;
- identify sources of funding for training activities;
- improve incident and emergency management effectiveness at state, regional and local levels; and
- undertake an annual assessment of previous activities with a review of the Framework every three years.

Given that a centralised emergency management exercise group is in place within the OESC, the aims of the *State Emergency Management Training and Exercising Strategic Framework* and the DPC's intention to adopt an "all hazards" approach to critical infrastructure protection arrangements in the revised CIP policy Framework, the Committee considers that there could be advantages in making greater use of the expertise available within the OESC in:

- assisting owners/operators of critical infrastructure in their general emergency planning preparedness; and

[339] Ms H. Silver, Secretary, Department of Premier and Cabinet, letter to the Committee, received 17 June 2011, p.14

- providing a central database for the recording of critical infrastructure protection exercises for analysis and dissemination of information to drive improvement.

This may also assist in addressing the comment made in the Auditor-General's report by Victoria Police that the CIPU does not have sufficient resources to enable the risk management plans of all critical infrastructure owners to be tested annually.[340]

Further, the DOJ has indicated to the Committee that whilst not seeking to replace existing mandated Part 6 training exercises, it considers that the OESC could provide a role in driving quality, accountability and improvement through testing the emergency preparedness of essential service operators.

The Committee is of the view that this is an area which could be investigated further through consultation between the DPC and the DOJ, with the involvement of Victoria Police and the OESC.

Recommendation 25:

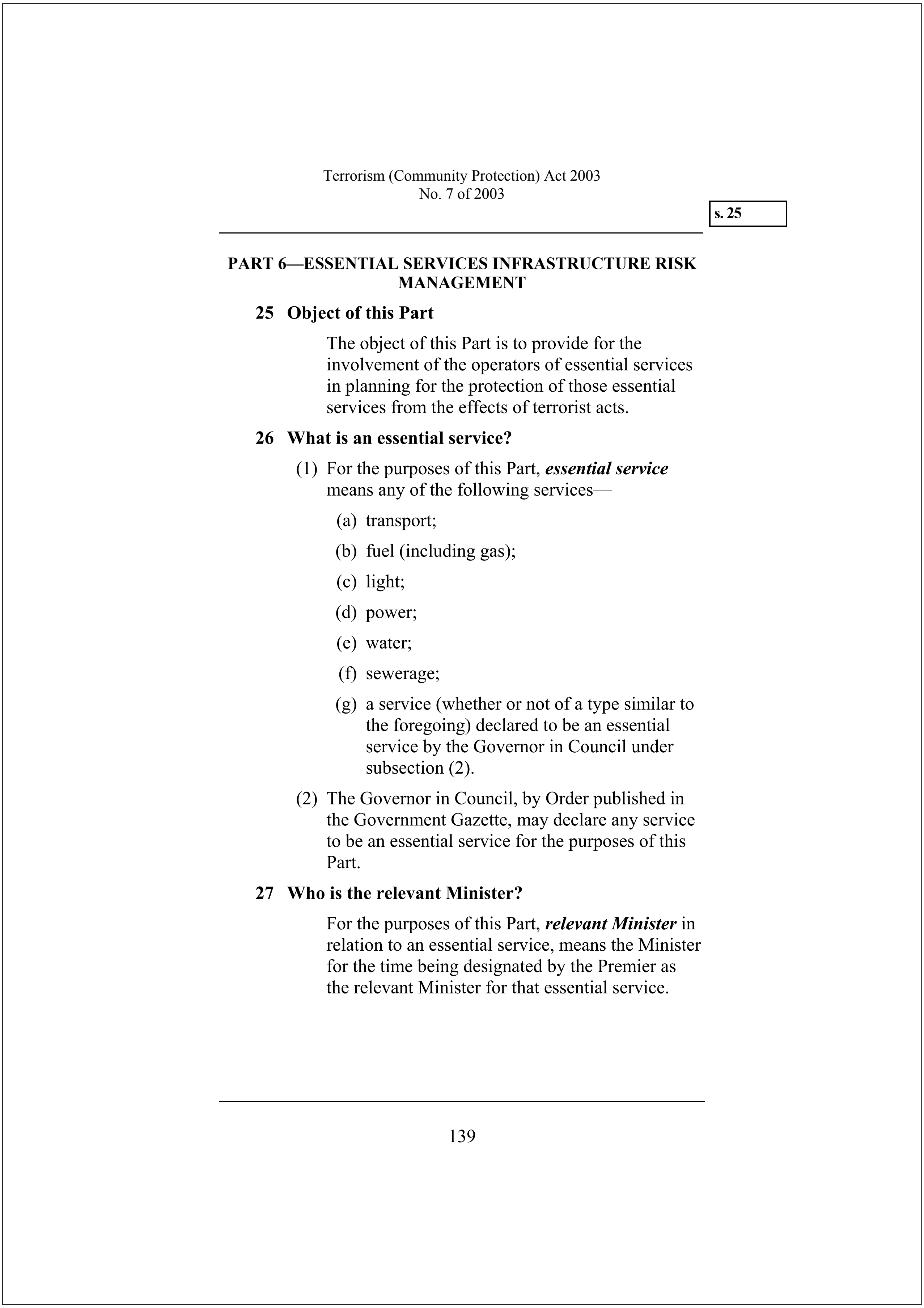
The Committee recommends that the Department of Premier and Cabinet together with the Department of Justice consider utilising the expertise of the Office of the Emergency Services Commissioner in developing and conducting training exercises to assist owners/ operators of critical infrastructure and essential services in validating their emergency management planning and preparedness to a range of risks/threats.

Recommendation 26:

The Committee recommends that Department of Premier and Cabinet together with the Department of Justice consider the option of the Office of the Emergency Services Commissioner providing a centralised database of critical infrastructure protection training exercises to enable central analysis to better identify and share improvement strategies.

[340] Victorian Auditor-General's Office, *Preparedness to Respond to Terrorism Incidents: Essential services and critical infrastructure*, January 2009, p.54

APPENDIX 1: TERRORISM (COMMUNITY PROTECTION) ACT 2003 – PART 6-ESSENTIAL SERVICES INFRASTRUCTURE RISK MANAGEMENT



PART 6—ESSENTIAL SERVICES INFRASTRUCTURE RISK MANAGEMENT

25 Object of this Part

The object of this Part is to provide for the involvement of the operators of essential services in planning for the protection of those essential services from the effects of terrorist acts.

26 What is an essential service?

(1) For the purposes of this Part, ***essential service*** means any of the following services—

(a) transport;

(b) fuel (including gas);

(c) light;

(d) power;

(e) water;

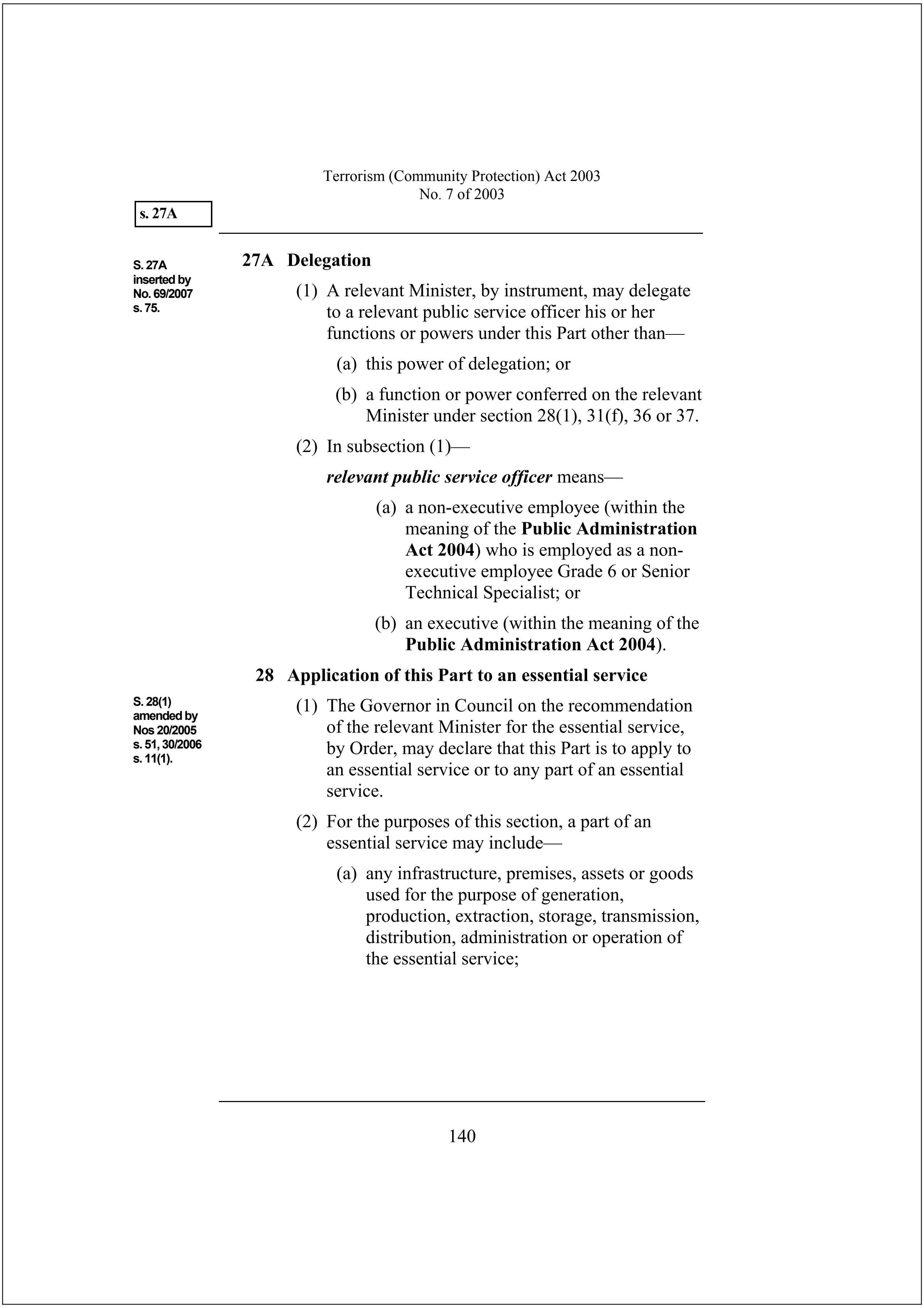
(f) sewerage;

(g) a service (whether or not of a type similar to the foregoing) declared to be an essential service by the Governor in Council under subsection (2).

(2) The Governor in Council, by Order published in the Government Gazette, may declare any service to be an essential service for the purposes of this Part.

27 Who is the relevant Minister?

For the purposes of this Part, ***relevant Minister*** in relation to an essential service, means the Minister for the time being designated by the Premier as the relevant Minister for that essential service.



S. 27A inserted by No. 69/2007 s. 75.

27A Delegation

(1) A relevant Minister, by instrument, may delegate to a relevant public service officer his or her functions or powers under this Part other than—

(a) this power of delegation; or

(b) a function or power conferred on the relevant Minister under section 28(1), 31(f), 36 or 37.

(2) In subsection (1)—

relevant public service officer means—

(a) a non-executive employee (within the meaning of the **Public Administration Act 2004**) who is employed as a non-executive employee Grade 6 or Senior Technical Specialist; or

(b) an executive (within the meaning of the **Public Administration Act 2004**).

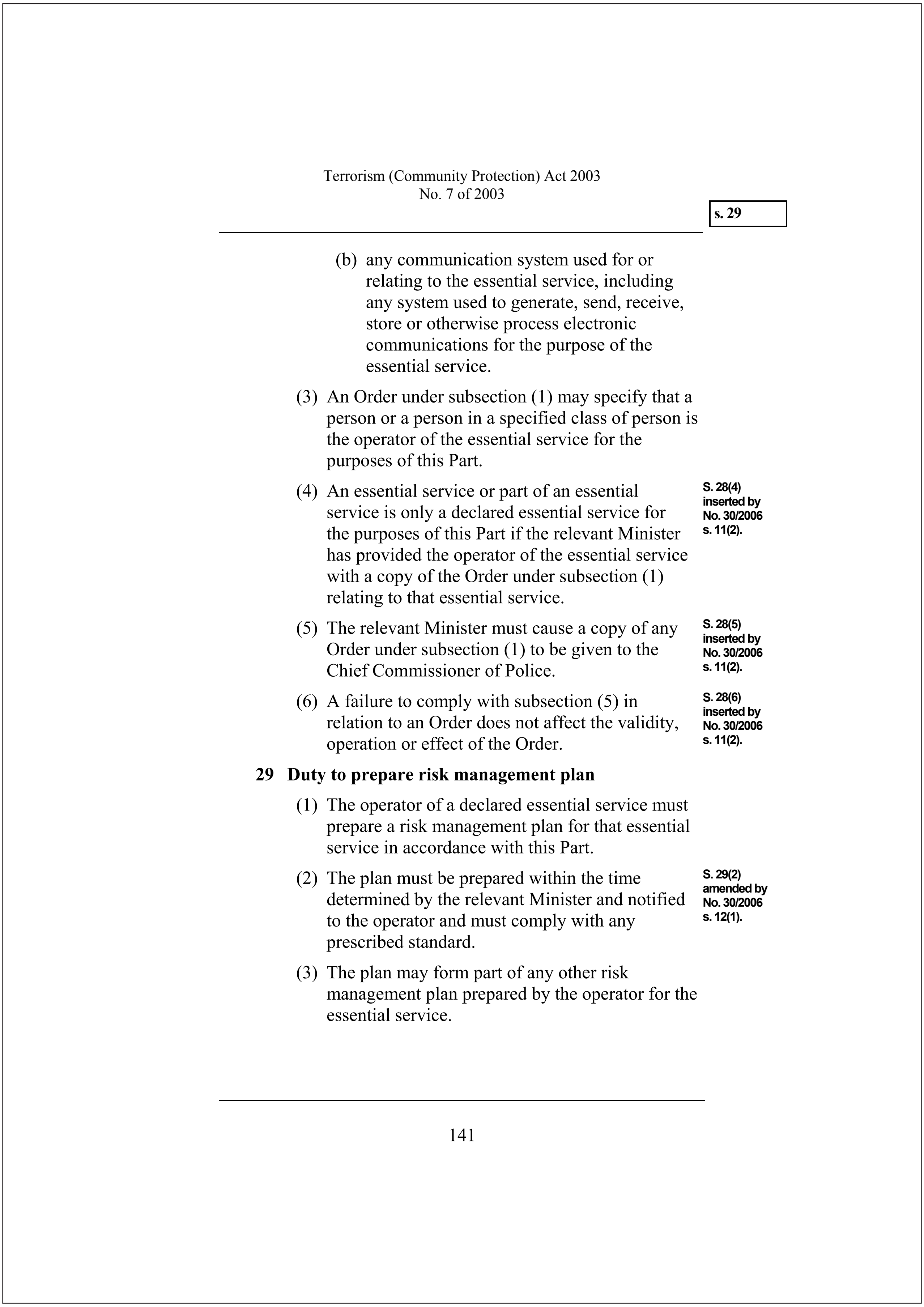
28 Application of this Part to an essential service

S. 28(1) amended by Nos 20/2005 s. 51, 30/2006 s. 11(1).

(1) The Governor in Council on the recommendation of the relevant Minister for the essential service, by Order, may declare that this Part is to apply to an essential service or to any part of an essential service.

(2) For the purposes of this section, a part of an essential service may include—

(a) any infrastructure, premises, assets or goods used for the purpose of generation, production, extraction, storage, transmission, distribution, administration or operation of the essential service;



(b) any communication system used for or relating to the essential service, including any system used to generate, send, receive, store or otherwise process electronic communications for the purpose of the essential service.

(3) An Order under subsection (1) may specify that a person or a person in a specified class of person is the operator of the essential service for the purposes of this Part.

S. 28(4) inserted by No. 30/2006 s. 11(2).

(4) An essential service or part of an essential service is only a declared essential service for the purposes of this Part if the relevant Minister has provided the operator of the essential service with a copy of the Order under subsection (1) relating to that essential service.

S. 28(5) inserted by No. 30/2006 s. 11(2).

(5) The relevant Minister must cause a copy of any Order under subsection (1) to be given to the Chief Commissioner of Police.

S. 28(6) inserted by No. 30/2006 s. 11(2).

(6) A failure to comply with subsection (5) in relation to an Order does not affect the validity, operation or effect of the Order.

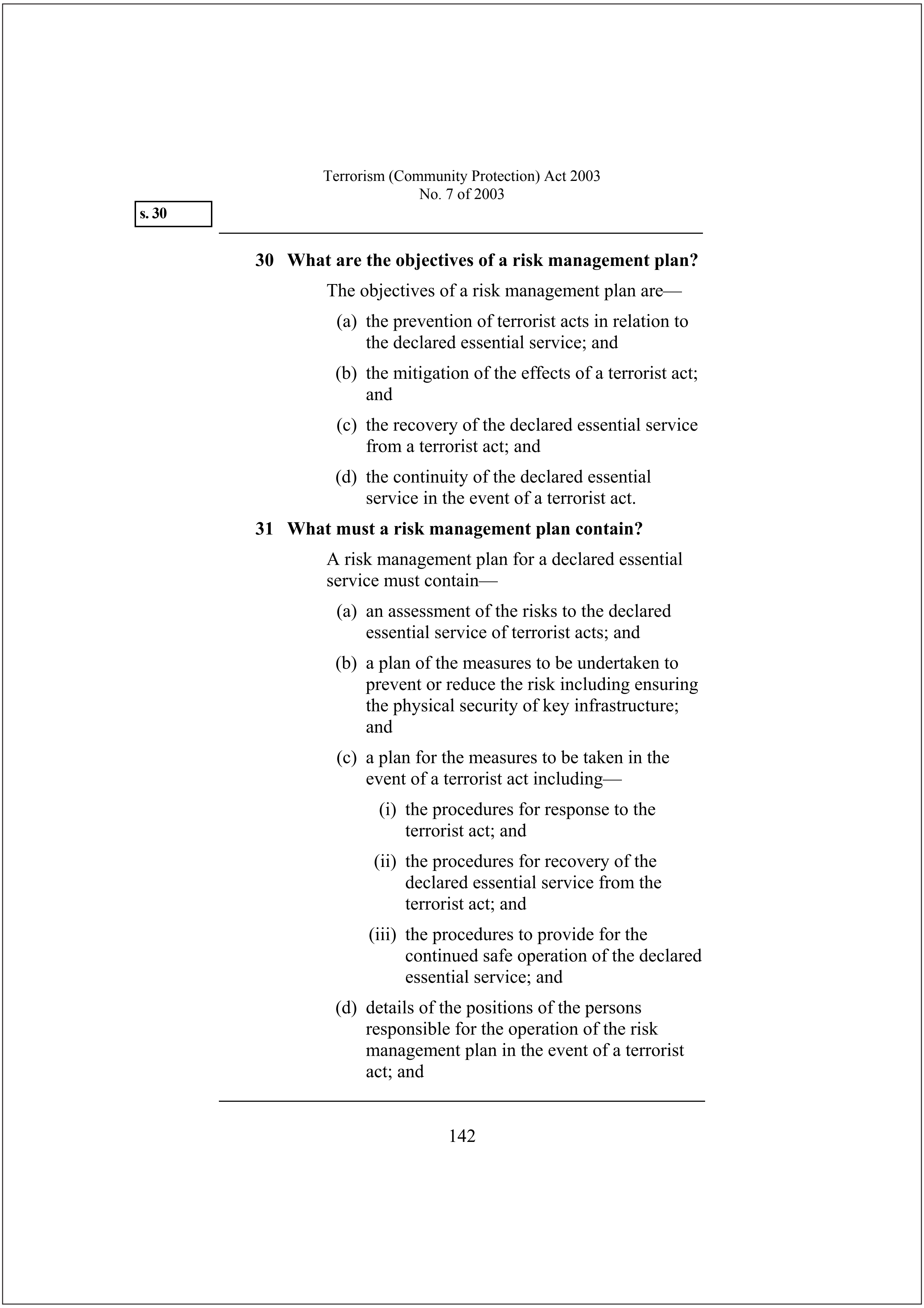
29 Duty to prepare risk management plan

(1) The operator of a declared essential service must prepare a risk management plan for that essential service in accordance with this Part.

S. 29(2) amended by No. 30/2006 s. 12(1).

(2) The plan must be prepared within the time determined by the relevant Minister and notified to the operator and must comply with any prescribed standard.

(3) The plan may form part of any other risk management plan prepared by the operator for the essential service.



30 What are the objectives of a risk management plan?

The objectives of a risk management plan are—

(a) the prevention of terrorist acts in relation to the declared essential service; and

(b) the mitigation of the effects of a terrorist act; and

(c) the recovery of the declared essential service from a terrorist act; and

(d) the continuity of the declared essential service in the event of a terrorist act.

31 What must a risk management plan contain?

A risk management plan for a declared essential service must contain—

(a) an assessment of the risks to the declared essential service of terrorist acts; and

(b) a plan of the measures to be undertaken to prevent or reduce the risk including ensuring the physical security of key infrastructure; and

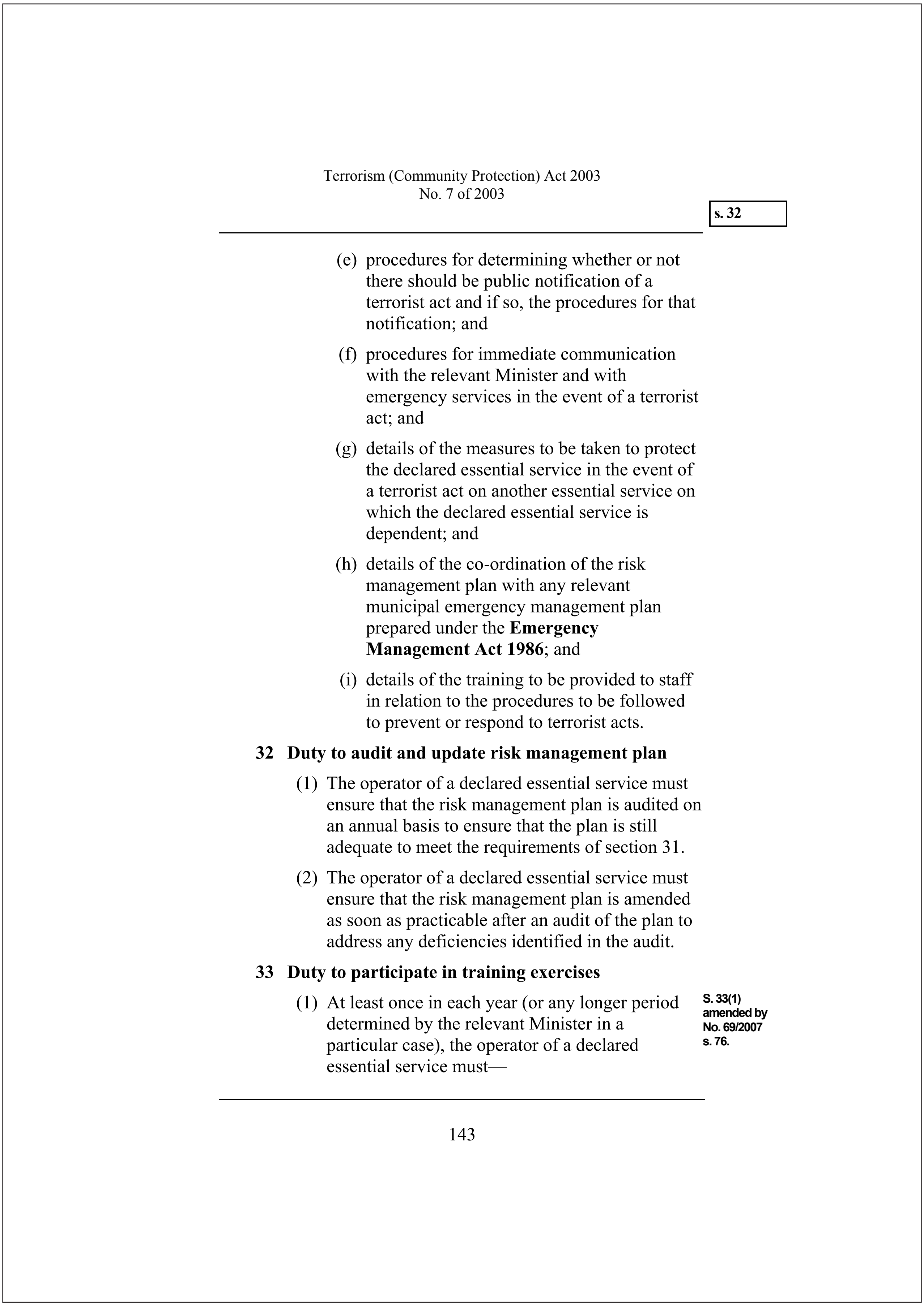
(c) a plan for the measures to be taken in the event of a terrorist act including—

(i) the procedures for response to the terrorist act; and

(ii) the procedures for recovery of the declared essential service from the terrorist act; and

(iii) the procedures to provide for the continued safe operation of the declared essential service; and

(d) details of the positions of the persons responsible for the operation of the risk management plan in the event of a terrorist act; and



(e) procedures for determining whether or not there should be public notification of a terrorist act and if so, the procedures for that notification; and

(f) procedures for immediate communication with the relevant Minister and with emergency services in the event of a terrorist act; and

(g) details of the measures to be taken to protect the declared essential service in the event of a terrorist act on another essential service on which the declared essential service is dependent; and

(h) details of the co-ordination of the risk management plan with any relevant municipal emergency management plan prepared under the **Emergency Management Act 1986**; and

(i) details of the training to be provided to staff in relation to the procedures to be followed to prevent or respond to terrorist acts.

32 Duty to audit and update risk management plan

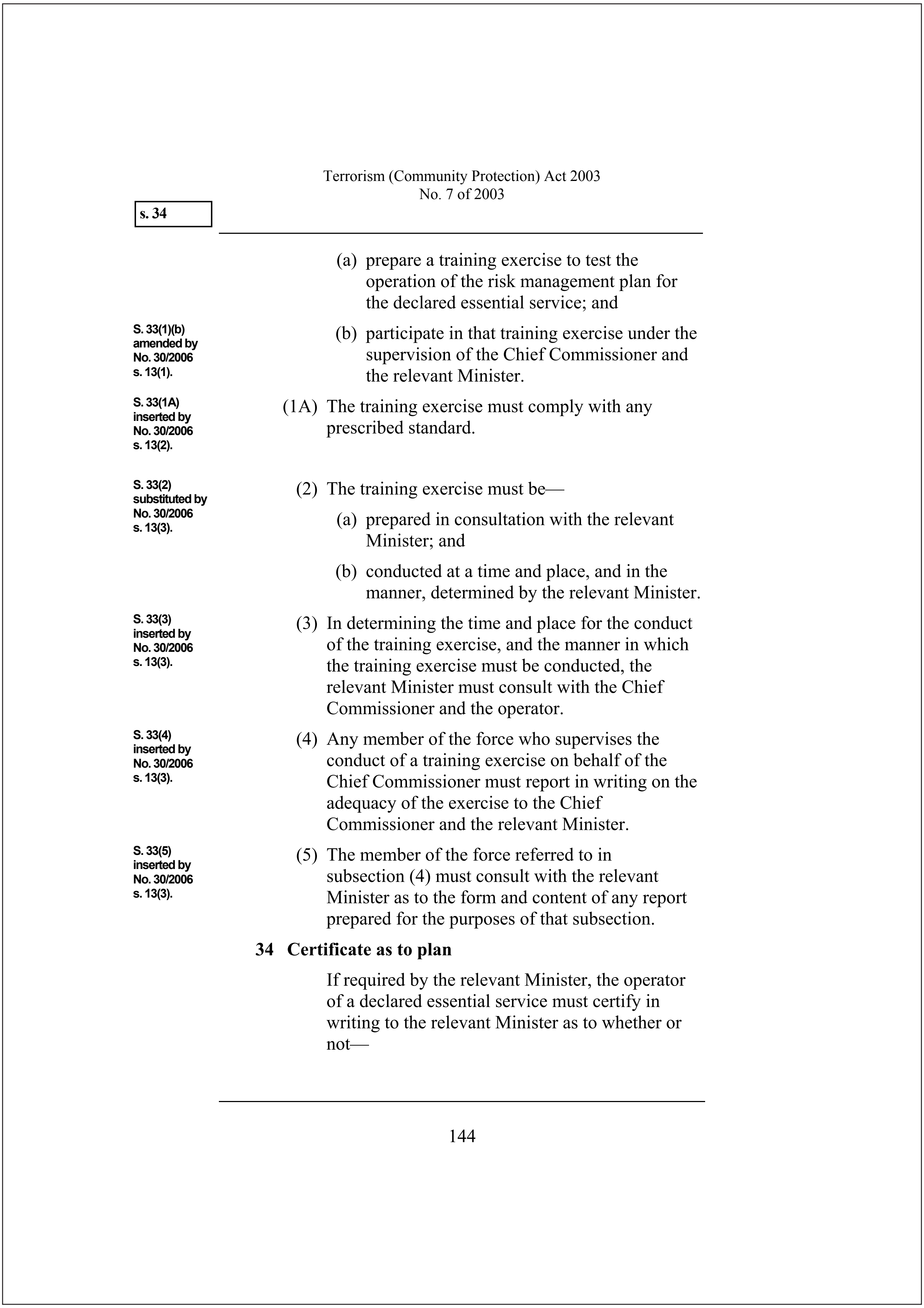
(1) The operator of a declared essential service must ensure that the risk management plan is audited on an annual basis to ensure that the plan is still adequate to meet the requirements of section 31.

(2) The operator of a declared essential service must ensure that the risk management plan is amended as soon as practicable after an audit of the plan to address any deficiencies identified in the audit.

33 Duty to participate in training exercises

S. 33(1) amended by No. 69/2007 s. 76.

(1) At least once in each year (or any longer period determined by the relevant Minister in a particular case), the operator of a declared essential service must—



Terrorism (Community Protection) Act 2003
No. 7 of 2003

s. 34

(a) prepare a training exercise to test the operation of the risk management plan for the declared essential service; and

S. 33(1)(b) amended by No. 30/2006 s. 13(1).

(b) participate in that training exercise under the supervision of the Chief Commissioner and the relevant Minister.

S. 33(1A) inserted by No. 30/2006 s. 13(2).

(1A) The training exercise must comply with any prescribed standard.

S. 33(2) substituted by No. 30/2006 s. 13(3).

(2) The training exercise must be—

(a) prepared in consultation with the relevant Minister; and

(b) conducted at a time and place, and in the manner, determined by the relevant Minister.

S. 33(3) inserted by No. 30/2006 s. 13(3).

(3) In determining the time and place for the conduct of the training exercise, and the manner in which the training exercise must be conducted, the relevant Minister must consult with the Chief Commissioner and the operator.

S. 33(4) inserted by No. 30/2006 s. 13(3).

(4) Any member of the force who supervises the conduct of a training exercise on behalf of the Chief Commissioner must report in writing on the adequacy of the exercise to the Chief Commissioner and the relevant Minister.

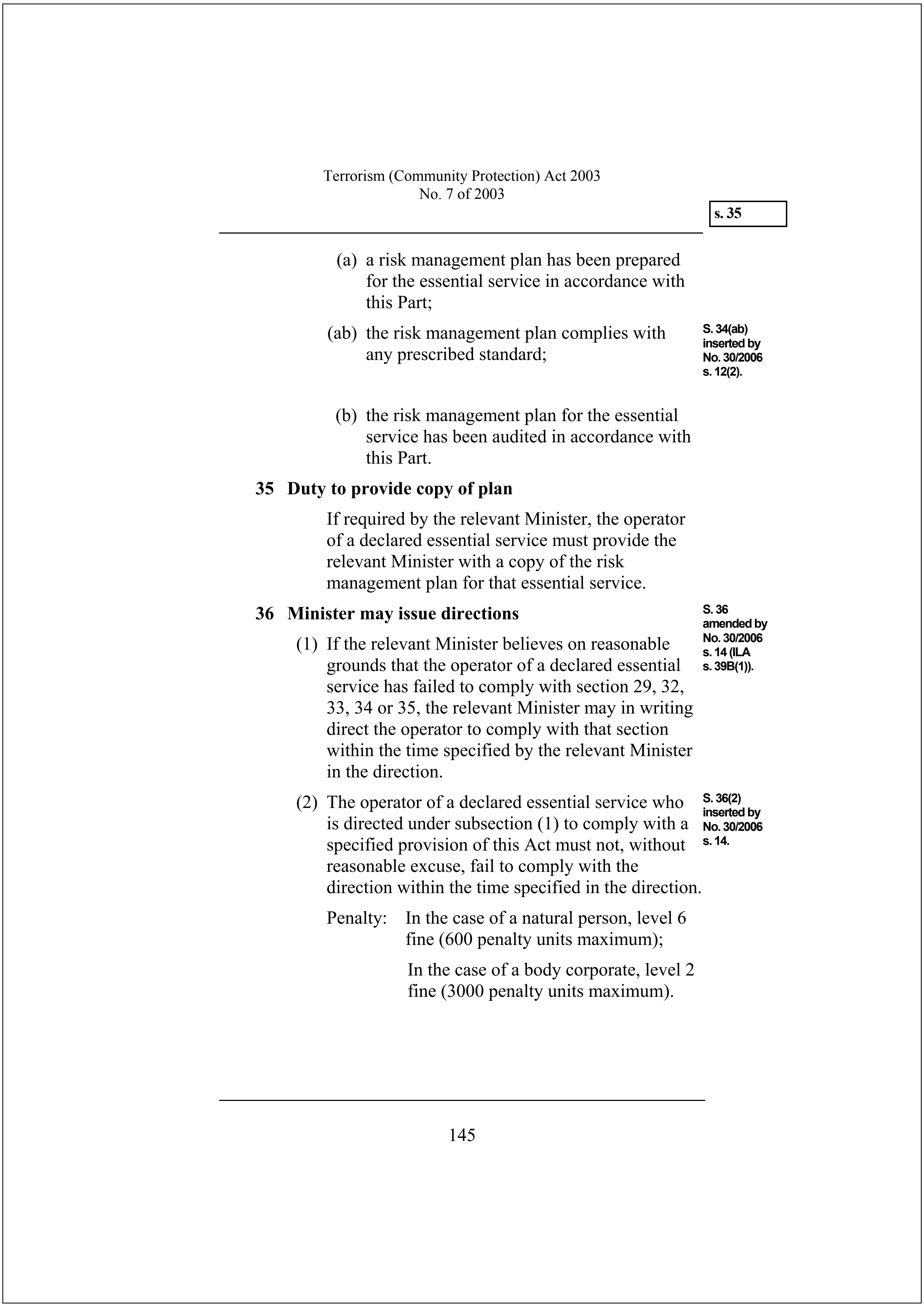
S. 33(5) inserted by No. 30/2006 s. 13(3).

(5) The member of the force referred to in subsection (4) must consult with the relevant Minister as to the form and content of any report prepared for the purposes of that subsection.

34 Certificate as to plan

If required by the relevant Minister, the operator of a declared essential service must certify in writing to the relevant Minister as to whether or not—

144



(a) a risk management plan has been prepared for the essential service in accordance with this Part;

S. 34(ab) inserted by No. 30/2006 s. 12(2).

(ab) the risk management plan complies with any prescribed standard;

(b) the risk management plan for the essential service has been audited in accordance with this Part.

35 Duty to provide copy of plan

If required by the relevant Minister, the operator of a declared essential service must provide the relevant Minister with a copy of the risk management plan for that essential service.

S. 36 amended by No. 30/2006 s. 14 (ILA s. 39B(1)).

36 Minister may issue directions

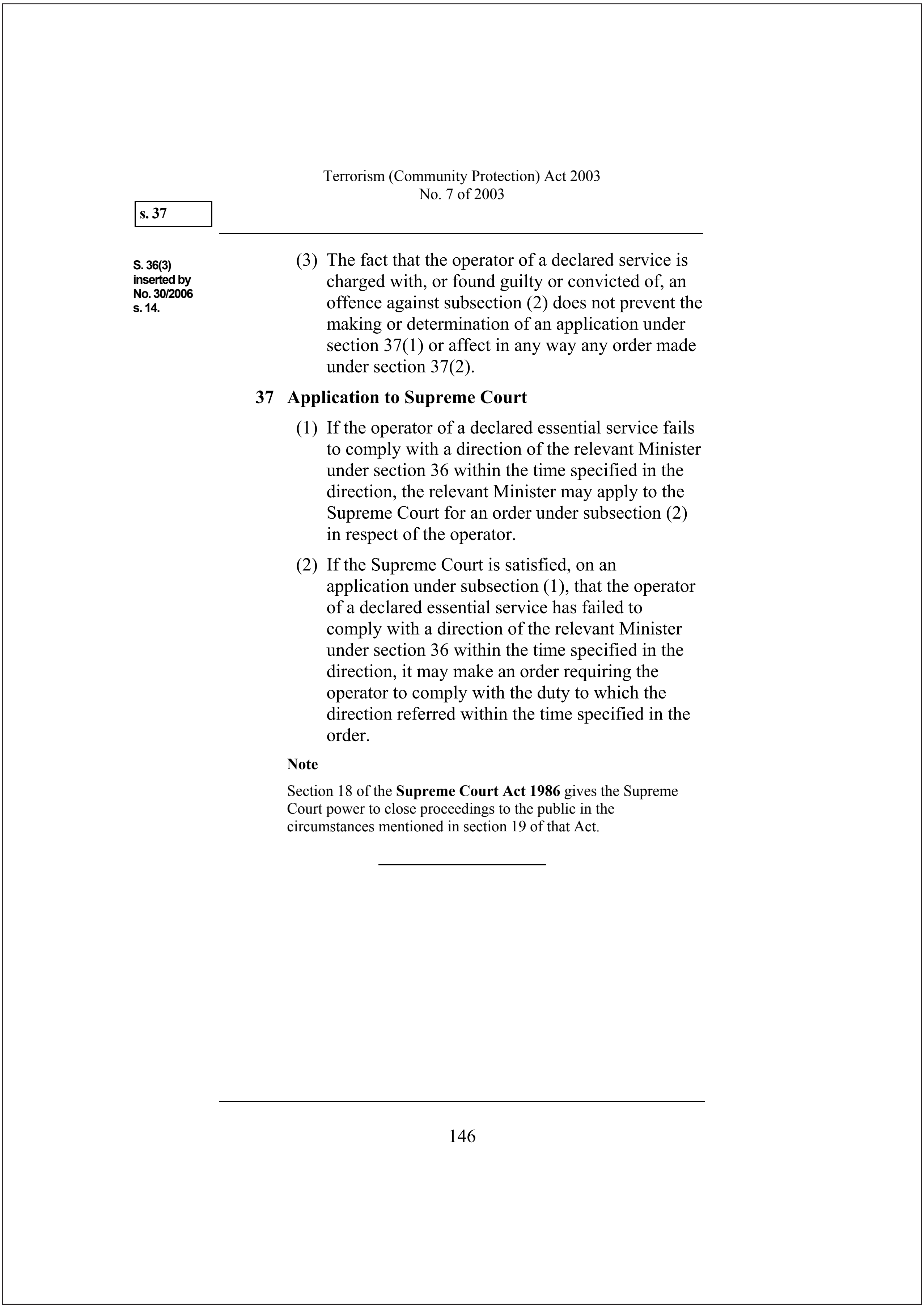
(1) If the relevant Minister believes on reasonable grounds that the operator of a declared essential service has failed to comply with section 29, 32, 33, 34 or 35, the relevant Minister may in writing direct the operator to comply with that section within the time specified by the relevant Minister in the direction.

S. 36(2) inserted by No. 30/2006 s. 14.

(2) The operator of a declared essential service who is directed under subsection (1) to comply with a specified provision of this Act must not, without reasonable excuse, fail to comply with the direction within the time specified in the direction.

Penalty: In the case of a natural person, level 6 fine (600 penalty units maximum);

In the case of a body corporate, level 2 fine (3000 penalty units maximum).



S. 36(3) inserted by No. 30/2006 s. 14.

(3) The fact that the operator of a declared service is charged with, or found guilty or convicted of, an offence against subsection (2) does not prevent the making or determination of an application under section 37(1) or affect in any way any order made under section 37(2).

37 Application to Supreme Court

(1) If the operator of a declared essential service fails to comply with a direction of the relevant Minister under section 36 within the time specified in the direction, the relevant Minister may apply to the Supreme Court for an order under subsection (2) in respect of the operator.

(2) If the Supreme Court is satisfied, on an application under subsection (1), that the operator of a declared essential service has failed to comply with a direction of the relevant Minister under section 36 within the time specified in the direction, it may make an order requiring the operator to comply with the duty to which the direction referred within the time specified in the order.

Note

Section 18 of the **Supreme Court Act 1986** gives the Supreme Court power to close proceedings to the public in the circumstances mentioned in section 19 of that Act.