Critical infrastructure protection

Source Policy

These Procedures and Guidelines support and must be read in conjunction with the following:

- VPMP Counter terrorism
- relevant parts of the Terrorism (Community Protection) Act 2003 (the Act)
- National Guidelines for Protecting Critical Infrastructure from Terrorism – 2011
- Victorian Framework for Critical Infrastructure Protection from Terrorism – 2007

Application

Procedures and Guidelines are provided to support the interpretation and application of rules and responsibilities. They include recommended good practices and assessment tools to help employees make lawful, ethical and professional decisions. Employees should use the **Professional and ethical standards** to inform the decisions they make to support interpretation of Procedures and Guidelines.

Procedures and Guidelines are not mandatory requirements on their own. However, where rules and responsibilities state that employees must have regard to Procedures and Guidelines, the Procedures and Guidelines must be used to help make decisions in support of the rules.

Procedures and Guidelines

1. Background

Since 2001, the Victorian Government has developed plans and arrangements to prevent and mitigate the effects of major disaster, particularly on the state's critical infrastructure. Protection of critical infrastructure is supported by the Victorian Framework for Critical Infrastructure Protection from Terrorism.

In addition to the framework, the *Terrorism (Community Protection) Act 2003* requires Essential Services that have been 'declared' to prepare a risk management plan and undertake an annual exercise to test the plan.

This guideline is designed to assist Victoria Police support the legislation and framework in meeting its requirements to protect the state's critical

infrastructure. Attached is a copy of the Critical Infrastructure classification table for information.

Criticality Table

Vital	Services are integral to the Victorian community and alternative services cannot be provided within the State. Loss or compromise will result in reliance on alternative services from outside Victoria.
Major	If services and/ or facilities are severely disrupted, major restrictions will apply and assistance may be required from outside Victoria.
Significant	Services and/ or facilities will be available but with some restrictions and/ or less responsiveness and/ or capacity compared to normal operation.
Low	Services and/ or facilities can be provided within Victoria with no loss of functionality.

2. Definitions

2.1 Critical Infrastructure

Critical infrastructure are 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.

Some examples of critical infrastructure are gas production facilities, bulk storage, pipelines and refineries of petroleum fuels, electricity generators and substations, dams, pumping stations and sewerage treatment plants, airports, sea lanes and shipping container facilities, health facilities, food supply, key government services and national icons.

2.2 Declared Essential Service

Declared Essential Services are those services that are indispensable to maintain the safety and wellbeing of the population at all times. An essential service is only a Declared Essential Service if the operator has been provided an Order by the Governor in Council declaring that the essential service or part of the essential service must comply with the requirements of Part 6, *Terrorism (Community Protection) Act 2003.*

Not all Declared Essential Services have critical infrastructure, and not all critical infrastructure are a Declared Essential Service.

3. Overview of Victoria Police role

Victoria Police has a role in infrastructure risk management of critical infrastructure sites in conjunction with their owner/operators in the following essential service sectors:

- banking and finance
- communications
- emergency services and government
- energy
- food supply
- health
- transport
- water
- any other service declared to be an essential service by the Governor in Council pursuant to part 6, *Terrorism (Community Protection) Act*.

4. Specific roles and responsibilities

4.1 Overview

While all members have the responsibility of reporting risks to critical infrastructure, the Critical Infrastructure Protection Unit (CIPU), Security and Organised Crime Intelligence Unit (SOCIU), Regional Emergency Management Superintendents (REMS), Local Area Commanders (LACs) and Station Commanders have specific roles within critical infrastructure protection which are outlined below.

4.2 Critical Infrastructure Protection Unit

Critical Infrastructure Protection Unit (CIPU) has a number of roles including liaison with State and Federal government agencies, critical infrastructure and Declared Essential Service owners and operators, and other agencies to:

- identify and assess those assets determined to be critical in terms of:
  - continuity of supply of essential services
  - their interdependency to other critical infrastructure and essential services
  - social and economic impact of loss or disruption to the asset or service
- conduct site assessments for new and changed critical infrastructure sites
- assist in the provision of protective security advice and development of protective security strategies to counter terrorism
- provide information relating to critical infrastructure sites to the REMS
- manage critical infrastructure information received from Station Commanders through Local Area Commanders and REMS

- provide critical infrastructure advice and interagency liaison to incident command in relation to all hazards response impacting on critical infrastructure or Declared Essential Services; and

- coordinate, supervise and evaluate annual exercises of Declared Essential Service owner/operators under Part 6, *Terrorism (Community Protection) Act*.

4.3 Security and Organised Crime Intelligence Unit

The SOCIU's role in relation to critical infrastructure protection is to:

- advise critical infrastructure owner and operators of relevant threat information in accordance with jurisdictional arrangements; and

- ensure that intelligence about critical infrastructure is gathered and disseminated to relevant agencies.

4.4 Regional Emergency Management Superintendents (REMS)

The REMS' role in relation to critical infrastructure protection is to:

- provide a coordination point within regions/divisions for monitoring critical infrastructure protection and emergency management response within their area of responsibility

- provide LACs with information relating to critical infrastructure sites in their area of responsibility

- monitor regional/LAC compliance and provide advice and information

- monitor and where required provide emergency management advice to critical infrastructure owner/operators in the development of their emergency management plans

- provide a regional coordinating role in the participation of appropriate operational police to participate in emergency management exercises, or supervise and evaluate exercises conducted by Declared Essential Services pursuant to Part 6, *Terrorism (Community Protection) Act*.

4.5 Local Area Commander

The Local Area Commanders' role in relation to critical infrastructure protection is to:

- oversee Station Commanders in their Police Service Area (PSA) conducting Site Update Reporting with critical infrastructure owner/operators a minimum of two times per year

- forward critical infrastructure Site Update forms to the REMS

- monitor information obtained from site contact reporting from Station Commanders to the REMS and CIPU

- monitor all hazards response planning and the tasking of patrols to critical infrastructure sites in their PSA by Station Commanders as appropriate, in particular during times of heightened terrorism alert.

4.6 Station Commander

The Station Commanders' role in relation to critical infrastructure protection is to:

- liaise with critical infrastructure owner/operators a minimum of two times per year in order to:
  - identify any changes to critical infrastructure at the site
  - record and store up to date details of the relevant site contact person on the critical infrastructure Site Contact Form (available on the CIPU Intranet page)
  - forward the critical infrastructure Site Contact Form to the LAC
- ensure familiarisation and awareness of any hazard/s at the site and mitigate any risk to the safety of members in any operational response to the site

- ensure the tasking of patrols in relation to critical infrastructure sites as appropriate, in particular during times of heightened terrorism alert

- where appropriate, ensure Field Contact Reports or Information Reports are submitted for all suspicious contacts or incidents relating to critical infrastructure sites or Declared Essential Services

- where requested, participate or arrange a delegate/s to participate in any emergency training exercise being organised and conducted by the owner/operator of critical infrastructure

- where requested by a REMS, participate or arrange a delegate/s to participate in any training exercise being organised and conducted by a Declared Essential Service owner/operator for their requirements pursuant to Part 6, *Terrorism (Community Protection) Act*.

Further assistance and advice is available through the CIPU intranet pages.

5. Information security

All information and intelligence relating to critical infrastructure must be stored according to its security classification. For further information and guidance consult;

- **VPMP Information categorisation, collection and recording**

- **VPMP Information use, handling and storage**
- **CIPU intranet site.**

Further Advice and Information

For further advice and assistance regarding these Procedures and Guidelines, and to access relevant site contact information and forms visit the CIPU intranet site or contact CIPU.

Update history

Date of first issue	**22/02/10**	
Date updated	**Summary of change**	**Force File number**
18/03/2013	Inclusion of further clarification into the roles of CIPU, SOCIU, REMS, Local Area and Station Commanders	066278/11
15/4/2013	Minor amendment to section 2 removing reference to civil infrastructure and replacing with critical infrastructure.	066278/11
18/11/2013	Correction of minor error in relation to the role of Regional Emergency Management Superintendents (REMS). References to redundant instruments following IMSSD review have been updated with corresponding new instruments.	066278/11 069562/11