



Australian Government

FACT SHEET



Trusted Information
Sharing Network
for Critical Infrastructure Protection

Critical Infrastructure Protection Modelling and Analysis Program

Overview

The Critical Infrastructure Protection Modelling and Analysis Program (CIPMA) Program is a world-leading computer modelling program. It is a key component of the Australian Government's efforts to enhance critical infrastructure protection and is a major national security initiative. It also supports the work of the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN).

CIPMA helps strengthen Australia's economic and social resilience by providing 'virtual insight' into disruptions to services whether caused by natural or human disasters. Owners and operators of critical infrastructure can use this information to plan how to prepare, prevent, respond to or recover from an adverse event. CIPMA also helps governments shape their policies on national security and critical infrastructure protection.

CIPMA has achieved good coverage of the banking and finance, communications and energy sectors and is progressing coverage of the water sector. The inclusion of transport, on which so much of our economy and community rely, will add to the picture of critical infrastructure interdependencies within and between different sectors. Data collection from the transport sector is expected to start in 2009. Inclusion of other key sectors in the CIPMA capability will occur over time.

Funding was provided in the 2008–09 Budget to move CIPMA from a pilot project to an operational program. CIPMA is already proving to be a valuable tool, having been used to support security planning for APEC Leaders' Week in September 2007 and World Youth Day in July 2008, and a range of other exercises and activities.

The Attorney-General's Department manages the CIPMA program and has engaged Geoscience Australia as the technical partner.

CIPMA's goals

CIPMA's primary goal is to strengthen national security and better protect Australia's critical infrastructure. It does this through a computer based capability which uses a vast array of data and information from a range of sources (including the owners and operators of critical infrastructure) to model and simulate the behaviour

and dependency relationships of critical infrastructure. The capability includes a series of ‘impact models’ to analyse the effects of a disruption to critical infrastructure services. The impact models assess the flow-on effects of a critical infrastructure service disruption within and across sectors, how the economy and population will be affected, how long the disruption is likely to last, the area affected and how the various infrastructure systems will behave as a result of the service interruption.

CIPMA is an ‘all hazards’ program, that delivers strategic support to government and business decision makers involved in critical infrastructure protection, counter-terrorism and emergency management, especially with regard to prevention, preparedness and planning, and recovery.

Specifically, CIPMA supports decision-making by helping to:

- identify connections between critical infrastructure nodes and facilities within sectors and across sectors
- provide insights into the behaviour of complex networks
- analyse relationships and dependencies
- examine the flow-on effects of infrastructure failure
- identify choke points, single points of failure, and other vulnerabilities
- assess various options for investment in security measures, and
- test mitigation strategies and business continuity plans.

Business-government partnership

The successful development of CIPMA is the result of an excellent partnership which has delivered strong support from a range of stakeholders, including the owners and operators of critical infrastructure, state and territory governments, and Australian Government agencies.

The Infrastructure Assurance Advisory Groups of the TISN and critical infrastructure owners and operators play a key role in the Program, especially in providing information, data and expert knowledge on the operation of the sectors. CIPMA enjoys especially strong support from the five sectors (banking and finance, communications, energy, water services and transport) currently engaged in the Program.

Data confidentiality

The Australian Government is committed to protecting the sensitive information provided by the owners and operators of critical infrastructure to the CIPMA Program. To this end a number of security measures have been put in place in accordance with the Australian Government's Protective Security Manual and a secure facility has been constructed to house the capability.

CIPMA tasking

To ensure the orderly 'tasking' of CIPMA and the appropriate and secure dissemination of the tasking results, the Attorney-General's Department has developed the CIPMA Tasking and Dissemination Protocols. The Protocols also ensure that the integrity and confidentiality of the data and models are safeguarded at all times.

Tasking is open to all stakeholders and is the process through which owners and operators of critical infrastructure can put forward operational questions they want answered through modelling and analysis. CIPMA is currently running scenarios for the communications, energy and banking and finance sectors. Modelling of the water services sector has commenced with the aim of starting scenario work for this sector in early 2009.

Applications under the Protocols should be made on the application form, which is available from www.tisn.gov.au or by emailing cipma@ag.gov.au.

CIPMA capability architecture and analysis workflow

CIPMA's capability architecture explains components in the Program in terms of scenarios, data and models, impact and recovery, and decision support.

The CIPMA Analysis Workflow diagram explains the workflow from a scenario event that impacts on people, buildings and infrastructure. It also covers economic impacts.

A limited number of DVDs showing how CIPMA works (running time approx 3 mins 30 secs) are currently available. These can be ordered by emailing cipma@ag.gov.au.

Key milestones

- May 2006—initial 'proof of concept' successfully demonstrated to over 150 key stakeholders.

- March 2007—work on the water sector commenced with a series of user requirements workshops.
- End 2007—process for ‘tasking’ the capability commenced with application rounds run every four months (application rounds close end October, February and June).
- March 2008—coverage of key aspects of the first three priority sectors completed.
- September 2008—transport named as fifth CIPMA sector.

More information about CIPMA is available from the Critical Infrastructure Protection Branch of the Attorney-General’s Department.

Phone: (02) 6272 7108

Email: cipma@ag.gov.au

Address:

Critical Infrastructure Protection Modelling and Analysis Program
Attorney-General’s Department
Critical Infrastructure Protection Branch
Robert Garran Offices
National Circuit
Canberra ACT 2600