TISN
FOR CRITICAL INFRASTRUCTURE RESILIENCE

FACT SHEET

CIPMA

Critical Infrastructure Program for Modelling and Analysis

Overview

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

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 prepare, prevent, respond to or recover from an adverse event. CIPMA also helps governments shape their policies on national security and critical infrastructure resilience.

CIPMA has achieved good coverage of the banking and finance, communications, energy, water and transport sectors. The Attorney-General's Department manages CIPMA and has engaged Geoscience Australia as the technical partner.

CIPMA's goals

CIPMA's primary goal is to strengthen national security and enhance the resilience of 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 resilience, counter-terrorism and emergency management.

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.

CIPMA (cont')

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 Sector Groups of the TISN and critical infrastructure owners and operators play a key role in CIPMA, especially in providing information, data and expert knowledge on the operation of the sectors. CIPMA enjoys 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 CIPMA. To this end CIPMA is housed in a secure facility and a number of other security measures have been put in place in accordance with the Australian Government's Protective Security Manual.

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.

The application form for tasking is available from www.tisn.gov.au or by emailing cipprojects@ag.gov.au

CIPMA capability architecture and analysis workflow

The capability architecture explains components of CIPMA 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.

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

P: 02 6141 2794

E: cipprojects@ag.gov.au