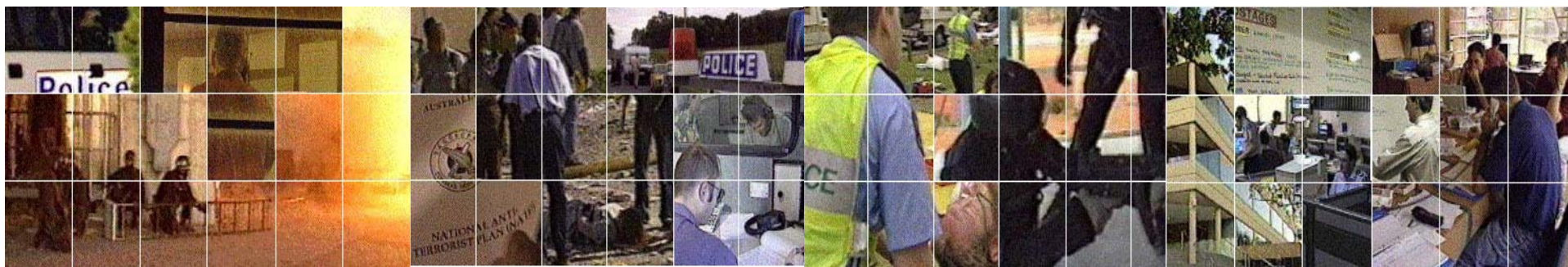# Government-Industry Collaboration:
An Australian Case Study

Steven Stroud
Director: Exercises, Projects & Review
e-Security Policy and Coordination Branch
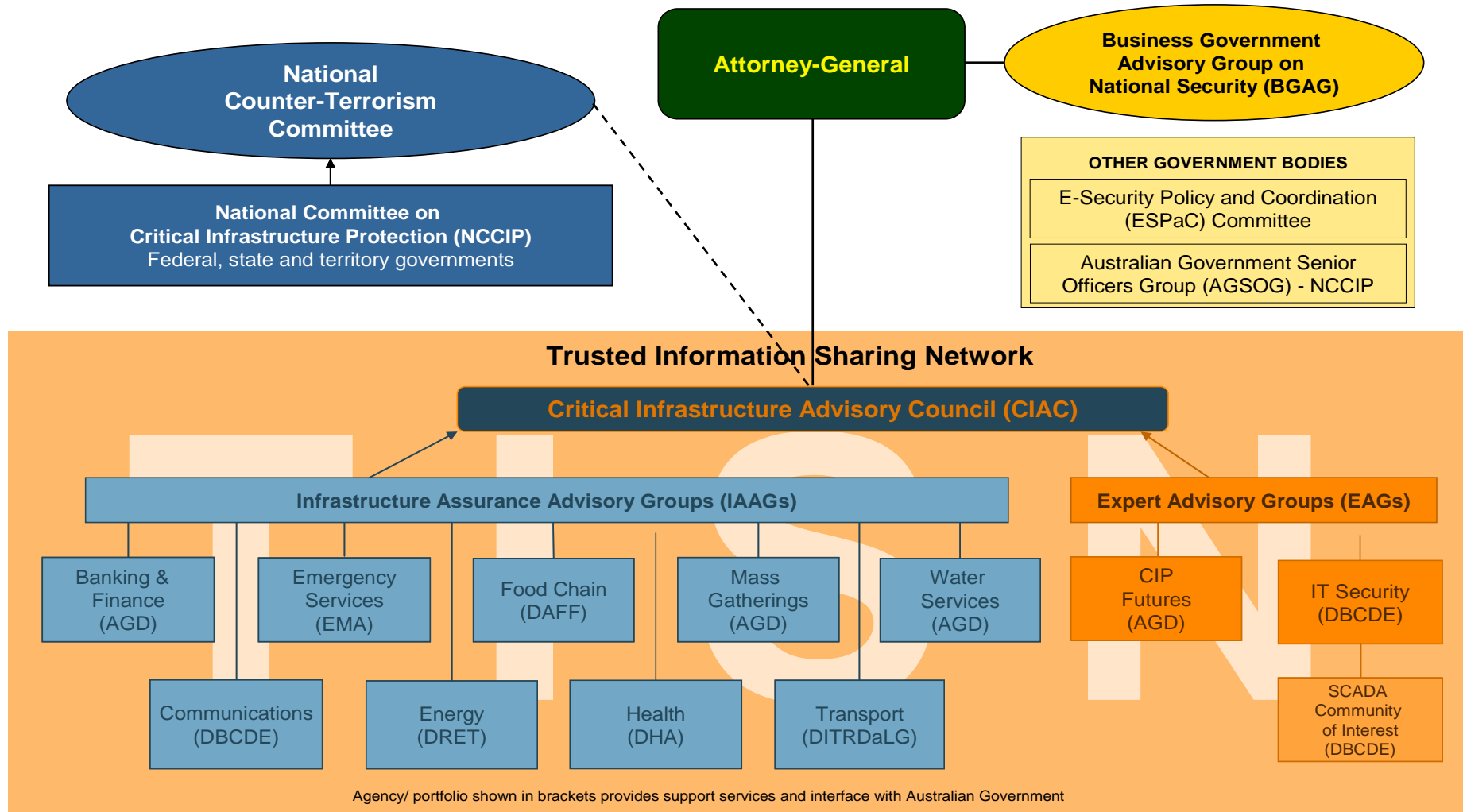
Role of Government

- To work with owners and operators of CI to:
  - ➤ Facilitate cooperation and information sharing.
  - ➤ Identify risks.
  - ➤ Develop suitable responses; and
  - ➤ Clearly set out roles and responsibilities.

The 'TISN'

Australia's Critical Infrastructure Protection Arrangements

National Counter-Terrorism Committee

Attorney-General

Business Government Advisory Group on National Security (BGAG)

National Committee on Critical Infrastructure Protection (NCCIP)
Federal, state and territory governments

OTHER GOVERNMENT BODIES

E-Security Policy and Coordination (ESPaC) Committee

Australian Government Senior Officers Group (AGSOG) - NCCIP

Trusted Information Sharing Network

Critical Infrastructure Advisory Council (CIAC)

Infrastructure Assurance Advisory Groups (IAAGs)

Expert Advisory Groups (EAGs)

Banking & Finance (AGD)	Emergency Services (EMA)	Food Chain (DAFF)	Mass Gatherings (AGD)	Water Services (AGD)	CIP Futures (AGD)	IT Security (DBCDE)

Communications (DBCDE)	Energy (DRET)	Health (DHA)	Transport (DITRDaLG)			SCADA Community of Interest (DBCDE)

Agency/ portfolio shown in brackets provides support services and interface with Australian Government

December 2007

E-Security National Agenda

- Reduce the e-security risk to Australian Government information and communications systems.

- Reduce the e-security risk to Australia's national critical infrastructure.

- Enhance the protection of home users and SMEs from electronic attacks and fraud.

Cyber Storm II

- AGD will also prepare for electronic incidents affecting critical infrastructure by coordinating and undertaking cyber exercises, including Australia's participation in international cyber exercises such as Cyber Storm.

Cyber Storm

- First truly national cyber exercise
- Largest Government sponsored cyber exercise of it's kind in Australia
- Incorporated various levels of government and private sector players

Aim

- Focuses on an event or cyber specific scenario that raises to the level of an Incident of National Significance

Who played

- 5 Infrastructure Sectors
  - Water, Energy, IT, Communications and Banking and Finance
- 2 State and Territory Governments
  - SA and WA
- 5 Countries
  - Australia, Canada, New Zealand, US and UK

Cyber Storm II

- Government provided the framework
- Opportunity for participating organisations to do an internal exercise at the same time
- Allows external communications channels to be practiced that would normally be notional

Planning

- 5 Phases
- Trusted Agent Agreement
- Portal
- Media

Planning

- Concept development
- Objectives
- Scenario development
- Walk through

Exercise Execution

- Included Law Enforcement and Intelligence build up of 2-4 weeks
- 3 days of Play
- 1 day Hot Wash
- Exercise Control

Exercise Control

Evaluation

- After Action Reports

Next Steps