The Australian Government's Approach to Submarine Cable Security

CIL-ICPC Workshop, Singapore, 15 April 2011

Michael Jerks, Assistant Secretary
Critical Infrastructure Protection Branch
Attorney-General's Department
Australia

Adam Cason, A/g Senior Lawyer
Infrastructure and Digital Economy Services
Department of Broadband, Communication and the Digital Economy
Australia

The protection of submarine cables in Australia

- There are two key components to the Australian Government's approach to submarine cable protection:
  - *Critical Infrastructure Resilience (CIR) Strategy; and*
  - *Regulatory protection and monitoring*

- This presentation will provide an overview of each of these components

What is Critical Infrastructure?

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.

Community expectations

- Community expects the Government to be engaged on issues that impact the nation

- Critical infrastructure (CI), 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

- Accordingly, the Australian Government is a key stakeholder in understanding the vulnerabilities and dependencies in and across CI

Australian Government's approach to CI

- The Australian Government generally takes a non-regulatory approach to critical infrastructure.

- Owners and operators of critical infrastructure are best placed to manage risks to their operations

- Certain sectors of critical infrastructure, however, are regulated to strengthen security of specific assets and to comply with international law and treaty obligations

Critical Infrastructure Resilience Strategy

- Launched by the Attorney-General in June 2010

Aim:

*"(The) continued operation of critical infrastructure in the face of **all hazards**, as this critical infrastructure supports Australia's national defence and national security and underpins our economic prosperity and social wellbeing"*

The shift away from protection to *resilience*

Critical Infrastructure Resilience Strategy

Foreseeable Risks	Unforeseen or Unexpected Risks
➢ Legal requirements ➢ Expand due diligence via information on risks/vulnerabilities etc ➢ Risk management approach ➢ Sector risk assessments etc	➢ Building capacity in organisations ➢ Enhanced adaptive ability ➢ Capturing learnings from incidents and near misses ➢ Body of knowledge on organisational resilience ➢ Dealing with complexity

Previous CIP Program

Business – Government Partnership

- A significant proportion of Australia's critical infrastructure is privately owned or operated
- Critical infrastructure resilience cannot be achieved by either Government or Industry alone
- Partnership required to share information, raise awareness of dependencies and vulnerabilities, and to facilitate collaboration to address any impediments

Trusted Information Sharing Network (TISN)

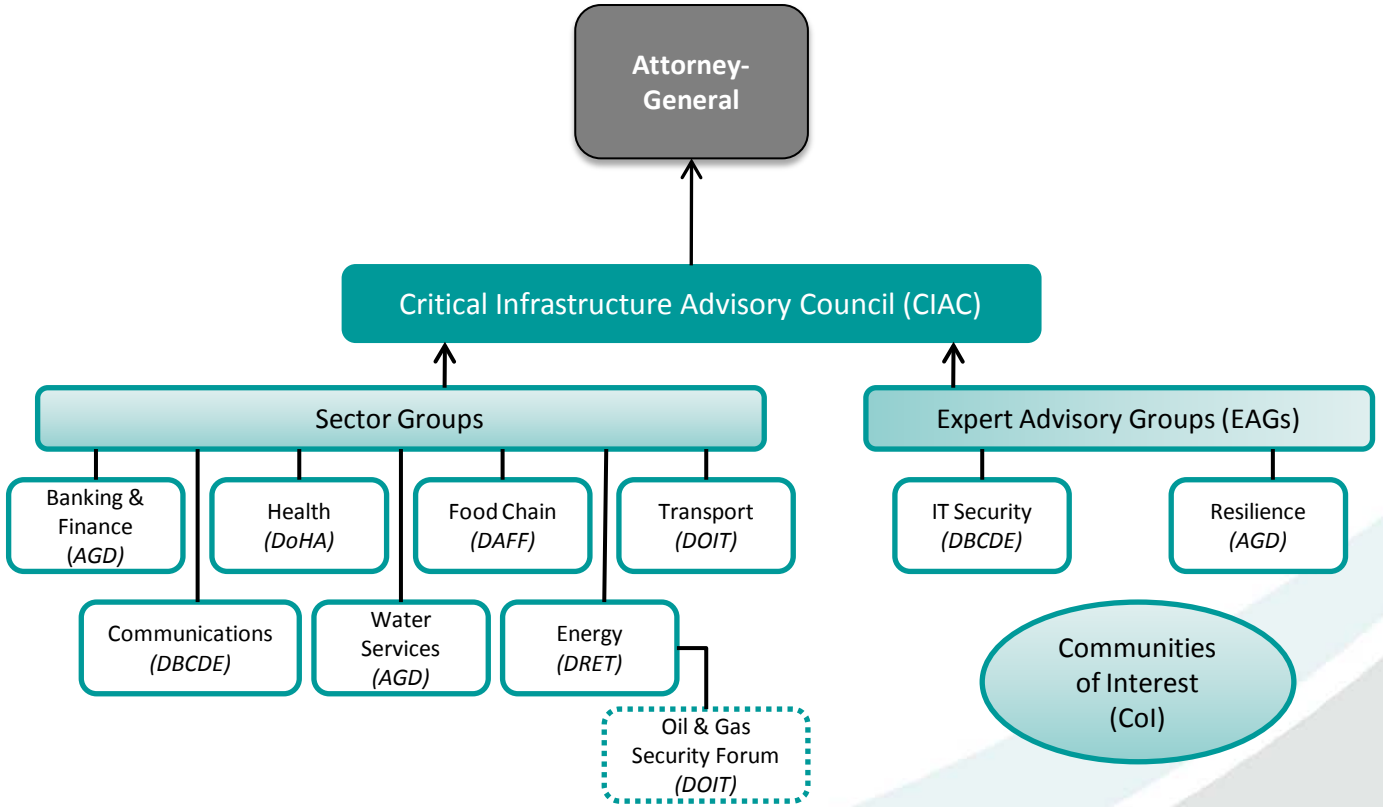
- The Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience is the most visible component of the Australian Government's business-government partnership.

- Forum in which the owners and operators of critical infrastructure work together and share information on threats and vulnerabilities and develop strategies and solutions to mitigate risk.

- The TISN operates on an all hazards basis, including terrorism, natural disasters, pandemics, accidents, cyber attack, criminal activity and negligence.

The Australian Government's Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience

TISN FOR CRITICAL INFRASTRUCTURE RESILIENCE



AGD	Attorney-General's Department	*DOIT*	Department of Infrastructure and Transport
DAFF	Department of Agriculture, Fisheries and Forestry	*DoHA*	Department of Health and Ageing
DBCDE	Department of Broadband, Communications and the Digital Economy	*DRET*	Department of Resources, Energy and Tourism

TISN Communications Sector Group (CSG)

- The CSG brings together owners and operators of Australia's critical infrastructure in:
  - *Telecommunications*
  - *International telecommunication submarine cables*
  - *Postal, and*
  - *Broadcasting sectors.*
- The CSG's purpose is to identify, analyse, discuss and share information on issues effecting the protection of Australia's critical communications infrastructure.

Why do submarine cables need to be protected?

- Australia is an island and relies on its undersea cable systems for almost all of its international communications connectivity

- Increasing use of the Internet and electronic services has accelerated demand for bandwidth

- A major disruption would have significant social, economic and security impacts

Submarine Cable Exercise (March 2009)

- The aim was to raise awareness of the implications of a major submarine cable incident

- A key objective of the exercise was to raise the awareness of the criticality of the submarine cable infrastructure on other critical infrastructure sectors and government.

- Complementary to the work of the ICPC

Submarine Cable Regulatory Regime

- Telecommunications in Australia are generally regulated by the *Telecommunications Act 1997.*

- The protection of submarine cables is provided by Schedule 3A of the *Telecommunications Act*, which was inserted into the Act in 2005.

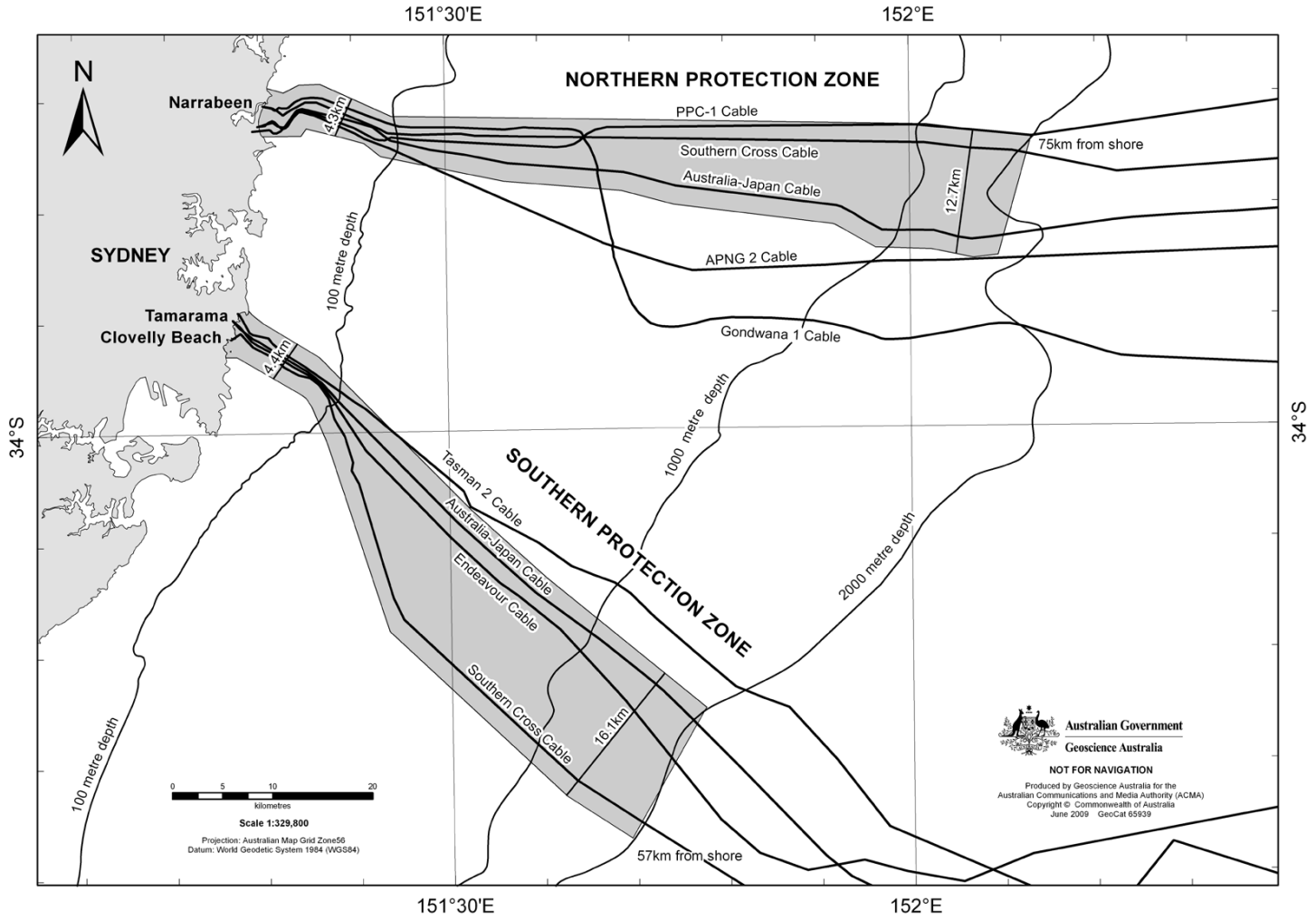
- The Australian Communications and Media Authority (ACMA) administers Schedule 3A

Schedule 3A of the Telecommunications Act

- Objectives
  - Security and reliability
  - Liability for compensation
  - Consistency & clarity with Commonwealth law

- Operation
  - Consultative committees
  - Protection zones
  - Awareness raising
  - Enforcement
  - Fines or imprisonment
  - Liability for damage
  - Permits

Example of Protection Zones



Sydney protection zones

2010 Review of Schedule 3A

- Recommendations
  - Monitoring and enforcement
  - Consultation processes for any new zones
  - Standard conditions
  - Interaction with UNCLOS
  - Protect cables wholly in Australian waters

- Recommendations being carefully considered
  - Response envisaged in the coming months
  - Need to avoid unnecessary regulation
  - Need to set a good regulatory example

Conclusions

- Damage to Australian submarine cables could have a severe impact on the economy and national security

- The Australian Government uses a mixture of regulatory and non-regulatory approaches to maximise the protection of submarine cables

- The Australian Government remains committed to submarine cable protection and resilience, and encourages international stakeholders to collaborate on submarine cable protection issues.

Further Information

Attorney-General's Department
www.ag.gov.au

Trusted Information Sharing Network
www.tisn.gov.au

Department of Broadband, Communications and the Digital Economy
www.dbcde.gov.au/broadband/protection_of_submarine_cables

Australian Communications Media Authority
www.acma.gov.au