The Australian Government’s Approach to Critical Infrastructure Resilience

GNSS Workshop
University of New South Wales
4 December 2013

Mr Kris Garred, Director
Critical Infrastructure Policy
Attorney-General’s Department
Presentation overview

- Critical infrastructure policy context
- Background and operation of the TISN
- Space infrastructure as critical infrastructure
The Australian and State and Territory Governments define critical infrastructure as:

“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.”
Role of the Government

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

– Failure in Critical infrastructure (CI) could impact our social or economic wellbeing and national security

– Accordingly, the Australian Government is a key stakeholder in assisting critical infrastructure providers increase their organisational resilience to ensure the continuity of essential services to businesses, governments and the community.
The non-regulatory approach

– The Australian Government generally takes a non-regulatory approach to critical infrastructure, with a focus on developing a strong business-government partnership

– Owners and operators of critical infrastructure are best placed to manage risks to their operations
Critical Infrastructure Resilience Strategy

Launched by the then A-G in June 2010

“(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”
1. Critical infrastructure owners and operators are effective in managing foreseeable risks to the continuity of their operations, through an intelligence and information led, risk-informed approach.

2. Critical infrastructure owners and operators enhance their capacity to manage unforeseen or unexpected risk to the continuity of their operations, through an organisational resilience approach.
The strategic imperatives

1. **Operate an effective business-government partnership with critical infrastructure owners and operators**

2. **Develop and promote an organisational resilience body of knowledge and a common understanding of organisational resilience**

3. **Assist owners and operators of critical infrastructure to identify, analyse and manage cross-sectoral dependencies**

4. **Provide timely and high quality policy advice on issues relating to critical infrastructure resilience**

5. **Implement the Australian Government’s Cyber Security Strategy to maintain a secure, resilient and trusted electronic operating environment, including for critical infrastructure owners and operators**

6. **Support the critical infrastructure resilience programs delivered by Australian States and Territories, as agreed and as appropriate**
Business – Government partnership

Why?

– 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 develop security solutions and address any impediments
Business – Government partnership

How?

– The Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience

– A forum in which the owners and operators of critical infrastructure work together to share security and resilience information

– 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)

Critical Infrastructure Advisory Council (CIAC)

- Sector Groups
  - Banking & Finance (AGD)
  - Health (DH)
  - Food Chain (DA)
  - Transport (DIRD)
  - Communications (DC)
  - Water Services (AGD)
  - Energy (DI)
  - Oil & Gas Security Forum (DIRD)

- Expert Advisory Groups (EAGs)
  - IT Security (DC)
  - Resilience (AGD)

Communities of Interest (CoI)

AGD: Attorney-General’s Department
DA: Department of Agriculture
DH: Department of Health
DIRD: Department of Infrastructure and Regional Development
DC: Department of Communications
DI: Department of Industry

www.ag.gov.au
Cross-sectoral dependencies

- CI networks and operations are becoming increasingly complex and interconnected.

- A disruption in one CI sector has the potential to significantly impact or disrupt other CI sectors leading to cascading failures.

- A cross-sectoral analysis of dependencies allows CI and the Government to understand system-wide risks that are beyond the purview of individual organisations or sectors.

- Australian Government undertake a number of activities to raise awareness of cross-sectoral dependencies, including conducting cross-sectoral exercises and workshops with industry and running the Critical Infrastructure Program for Modelling and Analysis (CIPMA).
Space infrastructure – where does it fit in?

**Space infrastructure is an important enabler of other critical infrastructure**

— “Space capabilities are increasingly important aspects of critical infrastructure assets, networks and supply chains.” — Australia’s Satellite Utilisation Policy

- Global Positioning System (GPS); Global Navigation Satellite System (GNSS); Position, Navigation & Timing (PNT)
- Satellite communications
- Earth observation

<table>
<thead>
<tr>
<th>Communications</th>
<th>Energy</th>
<th>Transport</th>
<th>Banking &amp; Finance</th>
<th>Health</th>
<th>Food &amp; Grocery</th>
<th>Water</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadband Satellite telephony</td>
<td>Exploration &amp; field development</td>
<td>GPS Vehicle &amp; cargo tracking</td>
<td>Transaction time stamping Network synchronisation</td>
<td>Emergency services guidance Rescue operations</td>
<td>Agriculture mapping Automated farm machinery</td>
<td>Meteorological Dam monitoring</td>
</tr>
</tbody>
</table>

**Space Infrastructure**
Cross-sectoral dependencies – space infrastructure

Disruption to GNSS Infrastructure

- Communications
  - Communication disruption
  - Timing systems
  - Multiple Sectors
- Energy
  - Resource exploration and drilling
  - Fuel disruption
  - Synchronisation of power grids
  - Power blackouts
  - Multiple Sectors
- Transport
  - Synchronisation of power grids
  - Power blackouts
  - Multiple Sectors
- Water
  - Geolocation and positioning
  - Security systems (vehicle tracking)
  - Supply chain interruption
  - Transport accidents
  - Customs tracking and coordination
  - Supply chains interruption
- Food and Grocery
  - Transport of foodstuff
  - Liquid fuel
- Multiple Sectors
  - Health supplies (i.e. pathology services)
- Health
  - Health
  - Chemicals
- Water
  - Flood monitoring and mitigation
  - Emergency preparation
  - Health
  - Banking and Finance
Space Community of Interest

Satellite Utilisation Policy

Principle 7: Protect and enhance national security and economic well-being.

‘The Australian Government will consider opportunities to establish a Space Community of Interest through the Trusted Information Sharing Network to bring relevant interested parties from industry, academia and government together to explore vulnerabilities, including interdependencies between space-related infrastructure and critical infrastructure, and to develop options to mitigate risk.

A Space Community of Interest has been established and will hold its first meeting in early 2014.

For further information on the Space Community of Interest please contact:
Joe Andrews - Space Coordination Unit - Department of Industry
Phone: 02 6213 6431
Email: joe.andrews@innovation.gov.au
Further information

Attorney-General’s Department
Web: www.ag.gov.au
Email: cir@ag.gov.au

Trusted Information Sharing Network
Web: www.tisn.gov.au
Questions?