Cyber Security and Critical Infrastructure Protection: An Australian Perspective

International Telecommunication Union
Regional Cybersecurity Forum for Asia-Pacific
September 2009

Duncan Anderson
Australian Government Attorney-General’s Department
Australia’s Digital Landscape: Snapshot

- **Australia’s digital economy**
  - 21.5 million population
  - 8.4 million active Internet subscribers
  - 7.3 million (87%) with ‘broadband’

- **National Broadband Network**
  - 100 mbps to 90% population

- **Increasing scale and sophistication of threats**
  - 17.7 million malware infections in 2008
  - 3,060 compromised computers per day
  - Annual cost of computer security incidents $595-$649 million

- **Top national security priority**
Australia’s Cyber Security Policy

• E-Security National Agenda
  - Secure and trusted operating environment for public and private sectors

• Priorities
  - Government systems
  - Critical infrastructure
  - Home users and small to medium enterprises

• Integrated with critical infrastructure protection strategy
  - Electronic, physical, personnel and procedural security
Trusted Information Sharing Network for Critical Infrastructure Protection (TISN)

Critical Infrastructure Advisory Council (CIAC)

Infrastructure Assurance Advisory Groups (Sector Based)
- Banking & Finance
- Emergency Services
- Food Chain
- Mass Gatherings
- Water Services
- Communications
- Energy
- Health
- Transport

Expert Advisory Groups
- CIP Futures
- IT Security
- SCADA Community of Interest

December 2007
Critical Infrastructure Protection Modelling and Analysis (CIPMA)

INFORMATION & DATA

SYSTEM MODELLING

DECISION SUPPORT

ECONOMIC
SOCIAL
INVESTMENT
BUSINESS CONTINUITY
SECURITY
RESILIENCE

ELECTRICITY
GAS
LIQUID FUELS
COMMUNICATIONS
BROADCASTING
BANKING & FINANCE
WATER
E-Security Review: Key Outcomes

• Cyber Security Operations Centre
  - Consolidated situational awareness
  - Coordinated operational response
  - Located within Defence Signals Directorate, with multi-agency expertise
  - Operational mid 2009

• New National CERT
  - Primary interface with private sector (systems of national interest)
  - Trusted information exchanges (communications, banking, SCADA)
  - Primary Australian contact in global CERT community
  - Amalgamating GovCERT.au and (selected) AusCERT functions
  - Operational early 2010
E-Security Review: Other Outcomes

• **Internet Gateway Consolidation**
  - Enhance security while maintaining redundancy
  - Broader work on security of government systems

• **Internet Service Provider Code of Practice**
  - Educate and protect users

• **International Engagement Strategy**
  - Incident response, legal frameworks and law enforcement cooperation, critical infrastructure protection, capacity building
  - Bilateral, regional, multilateral institutions
Future Directions

• **New Policy Framework**
  - Released later in 2009

• **Research and Development**
  - National Security Science and Innovation Strategy

• **Crisis Management Plan**
  - Cyber security incidents of national significance
  - Exercise Cyber Storm III
Conclusions

- Government leadership role, in partnership with business and the community (domestically and internationally)

- Integrated approach against ‘all hazards’ and interdependencies

- Security is an enabler to providing trusted and resilient systems
Questions?

Thank You

Duncan Anderson
Australian Government
Attorney-General’s Department

duncan.anderson@ag.gov.au