ITU REGIONAL CYBER SECURITY FORUM FOR ASIA-PACIFIC AND SEMINAR ON THE ECONOMICS OF CYBERSECURITY

WELCOMING ADDRESS BY KEITH BESGROVE

First Assistant Secretary

Telecommunications, Network Regulation and Australia Post

Department of Broadband, Communications and the Digital Economy

Good morning everyone, it is my great pleasure to welcome you all to the Regional Cybersecurity Forum for the Asia-Pacific and to the beautiful city of Brisbane. I am especially glad to welcome Mr Joon Yeon Hwang, the President and CEO of the KISA (the Korea Information and Security Agency of the Republic of Korea) and Dr Kim from the ITU Regional Office in Bangkok, who together with her very efficient officers have been responsible for organising this event.

As the internet's impact on economies and society continue to increase, there is an overwhelming need to ensure confidence and security in the use of ICTs and the internet.

The internet's capacity to stimulate innovation and growth has resulted in a highly inter-connected online environment – it crosses our personal lives and transactions, is global in nature, and its infrastructure has become critical to our economies and societies.

Consequently, policies affecting the internet can no longer be seen as narrow sectoral policies having to do with telecommunications only, but as mainstream economic and social policies reflecting the fact that the internet has become a fundamental economic and social infrastructure.

Along with these developments, the misuse of ICTs for criminal purposes is also increasing. Cyber attacks are becoming more sophisticated as cybercriminals become more organised, extending their operations beyond national borders. It is therefore vital that as policy makers and regulators we strive to become better connected and more organised than the criminals we are fighting.

Therefore the need to engage in developing better, more broad-based, governance arrangements and policies is now becoming a matter of increasing urgency and importance. This forum, therefore has an important role to contribute in this context and I thank the ITU for providing this opportunity.

Internationally as well as domestically, Australia has recognised the need to focus attention on e-security issues and believes in the need for an international approach to cyber security due to its borderless nature. Australia works collaboratively with international counterparts to effectively address these issues and actively participates in a range of international fora. This includes for example:

- **APEC** where Australia is a key driver of the security agenda and through the Security and Prosperity Working Group, is currently leading work on:
  - security issues associated with voice over internet protocol (VOIP) and wireless connections
  - submarine cable protection; cyber security awareness raising initiatives for home users, students and businesses
  - is also currently leading an APEC TEL initiative on awareness-raising across the region.
- The **OECD,** where Australia is actively engaged in measures to collaboratively address e-security risks.
  - Australia chairs the OECD Working Party on Information Security and Privacy (WPISP) where we work to develop policy options to sustain trust, information security and privacy in the global networked society.
  - As chair of this OECD Working Party, we have facilitated relationships between APEC TEL and the OECD and this has resulted in the APECTEL and the OECD working together on an analytical report on malware or malicious software.

The **ITU** has made it clear that security and confidence in the use of ICTs is a high priority and its range and diversity of activities in this context testify to this. For example:

- the ITU's work in the Telecommunication Standardisation Sector, which is studying and developing recommendations on this issue in Study Group 17.
- The ITU's Development sector, which is supporting developing countries to formulate Cybersecurity strategies and in this context is able to globally canvas attention and information sharing initiatives.
- The High Level Expert Group recently formulated by the ITU Secretary General Dr Hamadoun Toure to develop a GlobalCyber security Agenda provides further opportunities to study this issue in detail. The Global Cybersecurity Agenda is intended to provide a framework for international cooperation to enhance confidence and security in the information society. It will propose strategies for solutions and build on existing national and regional initiatives to avoid duplication of work and encourage collaboration amongst all relevant partners.

Given the borderless nature of e-security threats, this kind of international engagement to focus attention, build networks and share information and experiences is extremely important in developing and consolidating appropriate responses to cyber security threats.

From the point of view of a Member State, this is best done when organisations work within their areas of core competence, maintain a high degree of cooperation and information sharing both within their organisations, as well as with other organisations, in order to ensure efficiency and minimise the potential for duplication which would result in diluting the efforts that are being made.

This forum provides an opportunity for organisations and countries in the Asia-Pacific region to come together to share experiences, and work towards our common objective in promoting a culture of cyber security that will foster an inclusive, secure and global information society.