



MINISTER FOR HOME AFFAIRS
THE HON BOB DEBUS MP

Security in Government Conference 2008
National Convention Centre
Constitution Ave, Canberra
Wednesday 17 September 2008, 9.10am

CHECK AGAINST DELIVERY

[Acknowledgements]

First, may I acknowledge the traditional owners of the land we meet on –
and pay my respects to their elders, both past and present.

[Other Acknowledgements]

Chair – Mr Martin Studdert AM, Executive Director Protective Security
Coordination Centre, AGD
Distinguished guests
Ladies and gentlemen

For the most part, information technology is a positive tool which has become so integral to modern living it's pretty well indispensable.

But it's our increasing dependence on computers, the internet and mobile technologies and the valuable information they hold that increases opportunities and incentives for online crime.

The internet is now the target for traditional crimes such as fraud, identity theft and child exploitation.

And it's not just individuals – one of the largest potential threats to our security is sophisticated frauds and attacks against business, government and critical infrastructure, known as Technology Enabled Crime.

The Australian Government's e-security arrangements are coordinated through the Attorney-General's Department which works with a range of partners including the AFP, ASIO, the Defence Signals Directorate and the Department of Broadband and Communications.

The E-Security Review that you'll be hearing more about later this morning is a key Government initiative and without detracting from Marcella Hawkes' address, one of its main aims is to come up with a national framework that will secure Australia's electronic networks.

In other words, a system that government's, business and the community can use with the utmost confidence.

The Australian Federal Police, one of my Home Affairs portfolio agencies is up there with the best in the world for fighting online crime.

In March the AFP set up its High Tech Crime Operations unit which combined all of its technological capabilities, such as telephone and data interception and online policing, into the one area.

The unit is doing groundbreaking work and maximises the chances of detection, disruption and prosecution.

In June, the AFP announced the results of Operation Centurion which was the largest ever investigation ever conducted by the AFP into online child abuse.

Six months of work by 300 officers over 13,000 hours. Arrests conducted simultaneously by law enforcement authorities in 170 countries with 120 offenders identified in Australia alone.

Obviously it involved a high degree of cooperation both domestically and internationally and sharing information and exchanging technological advancements help everyone to counter high-tech crime.

The AFP also engages with peak industry bodies, such as the Australian Bankers Association, to combat and prevent banking fraud as part of the Joint Financial Investigations Team.

It's a partnership built around the co-location of staff from the financial sector and the AFP to ensure the sharing of information about online fraud.

There are approximately 450 phishing sites that target Australian financial institutions each month.

That translates into 5,000 sites designed to steal personal information which can then be used to steal money from private accounts.

The Australian Computer Emergency Response Team, or AusCERT as it's known and other government agencies work together to mitigate the impact of malicious software, such as viruses and Trojans, on individual, corporate and government systems.

According to AusCERT's Home Users Computer Security Survey of 2008, there are more than 20 million unique malicious software programs potentially impacting online consumers every year.

The Financial Investigations Team also works with internet service providers and international law enforcement agencies to reduce the impact of online banking fraud on Australian online consumers.

It identifies transnational criminal groups committing crimes against Australians and provides information to foreign law enforcement agencies to aid prosecutions overseas.

Domestically, the Financial Investigations Team, in conjunction with state and territory police services, undertakes prosecutions of individuals who help launder the proceeds of crime.

Just recently a Queensland woman was sentenced to eight months prison for her part in laundering approximately \$50,000 of fraudulently

obtained funds from an internet banking fraud.

The AFP is also a key member of the Anti-Phishing Working Group – a global industry and law enforcement association that's focused on eliminating fraud and identity theft.

In addition, the AFP has fostered relationships with key private sector organisations such as the United Kingdom Child Exploitation and Online Protection Centre, Telstra, Microsoft, MySpace, Google and several internet service providers.

A number of its members are based in London and Washington and an FBI attaché is on secondment in Canberra.

The Cybercrime Technology Information Network System, which allows information exchange for law enforcement agencies in the Asia region was developed by Japan's National Police Agency and is a secure, 24 hour a day IT network.

The AFP has access to this network, which allows the secure exchange and request of information with investigators and managers.

The AFP's also has member status of the Virtual Global Taskforce which in an alliance of law enforcement agencies from around the world working to fight child exploitation.

One of the biggest challenges ahead is to be as innovative and adaptive as the criminals being pursued.

It means ensuring the technology used to detect, prevent and investigate crime is as cutting edge and effective as ever.

Another major component of the AFP's High Tech Crime Operations is to raise awareness of the risks and show people how they can be either minimised, or avoided.

A very effective part of the AFP's prevention strategy is about engaging young people by appointing a youth advisor and creating a cyber safety youth forum.

The youth advisor helps officers use the right online language which provides credibility for online investigations that involve the exploitation of young people, such as grooming.

The Youth Forum got young people together to ask them how they'd like their online environment policed.

It means law enforcement activities can be contemporary and more effective.

The online environment is borderless so we have to be innovative, creative and continue strong partnerships with our international friends and allies.

The Australian Government and the AFP are well aware that our servant – information technology – has the potential to be exploited by those who seek to make it our executioner.

The Australian Government is making sure this won't be the case and will do all we can to keep our online environment safe and secure – and serving us well.

Thank you and I wish you all the best for today's deliberations as you address E-Security and the Cyber Environment.