SUBMISSION NO. 44

Australian Government

Attorney-General's Department

Attorney-General's Department

Submission to the House of Representatives Standing Committee on Communications Inquiry into Cyber Crime

July 2009

1 Introduction

The Attorney-General's Department (AGD) is the lead agency responsible for e-security policy across the Australian Government and is responsible for criminal law and law enforcement (including cyber crime). It is also the lead agency for identity security and critical infrastructure protection policy.

Australia's national security and economic and social wellbeing rely upon the use and availability of a range of information and communications technologies (ICT). Such systems include desktop computers, the Internet, mobile communication devices and other computer networks. As these systems and technologies become more pervasive, government, business and individuals are becoming more dependent on them for a range of purposes. Whether it is transacting online to purchase goods or services, communicating with others, managing finances, searching for information, or controlling the largest equipment in the mining or manufacturing industry, computers and computer-based communications are everywhere.

Criminal activity is often founded on the use of false or multiple identities. The capacity to accurately and efficiently verify that a person is who they claim to be is essential to protect Australians from identity theft and serious crimes, including organised crime and terrorism. Secure electronic identity management is, with e-security, an important element in protecting the Australian government, private sector and community against attacks launched using fraudulent access to computer networks.

In Australia, organisations and individuals regularly communicate and store items of great value in electronic form. Our identities, financial details, private communications, corporate and government secrets, and our creative and academic efforts all now reside within and travel through our ICT systems. Unfortunately, as the quantity and value of the content has increased so too have the efforts of criminals and other malicious actors, who have begun to turn to the Internet as a more anonymous, convenient and profitable way of carrying out their activities. Additionally, ICT, whether it be connected to the Internet or not, is vulnerable to exploitation by actors seeking to illegally and covertly obtain information for various reasons.

A number of Australian Government agencies are involved in Australia's efforts to combat cyber crime. Of particular relevance to this Inquiry are law enforcement agencies, including the Australian Federal Police (AFP), who are making a separate submission to the Inquiry detailing their activities in this area.

However, cyber crime is not just an issue of law enforcement; cyber crimes are not just committed by criminals per se. They may also be committed by others including nation states, and politically motivated groups (including terrorists). Actions taken by these actors, in addition to being cyber crimes, may also constitute acts of war, espionage or terrorism. These actors, and their actions, are not simply issues of criminality. They are also potential threats to Australia's national security and defence, in addition to our economic and social wellbeing. It is for this reason that measures to combat cyber crime fall within the broader ambit of Australia's e-security efforts. The Australian Government's e-security program has a broad mandate to consider issues on the prevention, preparedness, response and recovery (PPRR) relating to e-security threats, and Australian Government activities are targeted across the spectrum. It is for this reason that this submission outlines the broad context and detail of the Australian Government's and AGD's e-security policy and programs.

1.1 What is cyber crime?

The term ‘cyber crime’ refers to the type of criminal activity covered by the offences contained in Part 10.7 of the *Criminal Code Act 1995* (Cth) (Criminal Code). These relate to crimes that are committed directly against computers or computer systems and associated technologies, including the unauthorised access or impairment of computers.

1.2 Cyber crime and the online environment

As previously identified, ICT has become an even more integral part of almost every aspect of our lives including the delivery of essential services, commerce, banking and finance, health care, logistics and even the way in which we socialise and interact with each other. Continuing technological breakthroughs fuelled by an ever increasing worldwide demand for fast and massive data transfers and unlimited connectivity options will only continue this trend into the future. The last few years have seen remarkable increases in the level of access to ICT infrastructure, developments of new applications and devices and changing behavioural patterns of consumers.

The ICT environment for Australian government, business, industry, academia and home users operate is subject to a broad range of threats. The threats can come from a variety of sources including nation states, organised crime groups and networks, politically or religiously motivated groups (including terrorists), and issue motivated groups.

The motivations of these threat sources are as wide and varied as the sources. Notably, in relation to criminal organisations and individuals, they are:

- accessing sensitive government and private sector information for strategic and economic gain
- accessing personal identification and financial information for criminal and other purposes, and
- causing disruption in order to draw attention to a cause or for other reasons.

It is likely that in the near future we will see an escalation in interest from criminals seeking ways to benefit from conducting illegal activities online

2 Australian Government arrangements

2.1 Legal framework

2.1.1 Relevant offences in the Commonwealth Criminal Code

Parts 10.6 and 10.7 of the Criminal Code contain comprehensive offences dealing with the misuse of telecommunications and cyber crime. A detailed list of the relevant offences in these parts is at **Attachment A**. This attachment also includes a summary of relevant investigative powers under the *Crimes Act 1914* (Cth).

Part 10.6 contains offences that criminalise the inappropriate use of telecommunications, including the Internet. These offences include: using a carriage service to menace, harass or cause offence; threats to kill or cause harm to a person; and using a carriage service for child pornography.

Conduct such as online bullying, stalking and fraud could be covered by the offences in Part 10.6 of the Criminal Code.

Part 10.7 of the Criminal Code contains offences that criminalise conduct which impairs the security, integrity and reliability of computer data and electronic communications. These offences include: unauthorised access, modification or impairment with intent to commit a serious offence; unauthorised impairment of electronic communication; and unauthorised access to, or modification of restricted data. The offences in Part 10.7 were framed in general and technology neutral language to ensure that, as technology evolves, the offences will remain applicable. For example, the term 'computer' was not defined to ensure the computer offences will encompass new developments in technology, for example, mobile phones that allow access to the Internet. Conduct such as hacking into a person's Facebook account and altering it or using malicious software to steal personal information would generally be covered by the offences in Part 10.7 of the Criminal Code.

2.1.2 New identity theft offences

On 23 February 2009 the House of Representatives passed the Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2008. The Bill is expected to be debated in the Senate in the second half of this year. The Bill implements the model identity crime offences and victims' certificate provisions recommended by the Model Criminal Law Officers' Committee.

The Bill inserts three new identity crime offences into new Part 9.5 of the Criminal Code. With the exception of South Australia and Queensland, it is not currently an offence in Australia to assume or steal another person's identity, except in limited circumstances.

2.1.3 Cyber-terrorism offences

The Australian Government does not have a specific definition of the term 'cyber-terrorism'. However, the definition of 'terrorist act' in section 100.1 of the Criminal Code would cover activity of this nature. Section 101.1 of the Criminal Code provides that a person commits an offence if they engage in a terrorist act.

In accordance with the Criminal Code, a terrorist act has three elements, outlined below.

Firstly, it means an action or threat of action where the action or threatened action:

(a) causes serious harm that is physical harm to a person, or

(b) causes serious damage to property, or

(c) causes a person's death, or

(d) endangers a person's life, other than the life of the person taking the action, or

(e) creates a serious risk to the health or safety of the public or a section of the public, or

(f) seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to:

    (i) an information system, or

    (ii) a telecommunications system, or

    (iii) a financial system, or

(iv) a system used for the delivery of essential government services, or

(v) a system used for, or by, an essential public utility, or

(vi) a system used for, or by, a transport system.

However, such action or threat of action is excluded from the definition if it is advocacy, protest, dissent or industrial action and is not intended to:

(i) cause serious harm that is physical harm to a person, or

(ii) cause a person's death, or

(iii) endanger the life of a person, other than the person taking the action, or

(iv) create a serious risk to the health or safety of the public or a section of the public.

Secondly, to fall within the scope of the definition there is a requirement that the action is done or the threat is made with the intention of advancing a political, religious or ideological cause.

Thirdly, the action is done or the threat is made with the intention of either (a) coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country, or of part of a State, Territory or foreign country; or (b) intimidating the public or a section of the public.

In addition to the offence of committing a terrorist act, a number of the terrorist offences under the Criminal Code can be conducted with, or facilitated through use of the Internet, including recruiting or fundraising for a terrorist organisation, or receiving training in order to conduct a terrorist act.

2.2 Current e-security arrangements

The Australian Government's e-security programs are delivered by a number of Australian Government agencies, including:

- **Attorney-General's Department (AGD)** is responsible for developing Australian Government protective security policy and criminal justice. It is the lead policy agency for e-security and takes a leadership role in advancing business-government partnerships and providing e-security guidance to owners and operation of critical infrastructure and other systems of national interest. It also has responsibility for criminal law and law enforcement including administration of the Criminal Code.
- **Australian Communications and Media Authority (ACMA)** is responsible for regulation of broadcasting, the Internet, radiocommunications and telecommunications. As part of its role it gathers evidence and assists in protecting Australians from computer fraud and identity theft.
- **Australian Federal Police (AFP)** enforces Commonwealth criminal law and protects Commonwealth and national interests from crime in Australia and overseas. As part of its role it provides a specialised investigative capacity to support the identification and investigation of complex technology enabled crime offences, in partnership with the Australian law enforcement community. The AFP also collaborates with international agencies to address technology enabled crime issues.
- **Australian Government Information Management Office (AGIMO)** works with Australian Government agencies to ensure the productive application of ICT.

- **Australian Security Intelligence Organisation (ASIO)**'s responsibilities are defined by the *Australian Security Intelligence Organisation Act 1979*, including investigating electronic attacks conducted for purpose of espionage, sabotage, terrorism, or other forms of politically motivated violence, attacks on the defence system and other matters that fall under the heads of security in the *ASIO Act*.
- **Defence Signals Directorate (DSD)** is the national authority on the security of ICT across government, including threats posed to government ICT by cyber crime.
- **Department of Broadband, Communications and the Digital Economy (DBCDE)** is responsible for creating an environment that allows Australians to take full advantage of the opportunities offered by the digital economy. It works with industry and the community to raise awareness of e-security risks, including the risk of cyber crime, with a view to improving their online practices and behaviours.

The Australian Government approach to e-security is currently informed by the E-Security National Agenda (ESNA). The ESNA was established in 2001 and reviewed in 2006. The ESNA has three main objectives which are to:

- reduce the e-security risk to Australian Government information and communications systems
- reduce the e-security risk to Australia's national critical infrastructure, and
- enhance the protection of home users and small and medium enterprises from electronic attacks and fraud.

2.3 Review of arrangements

Since the 2006 review there have been a number of significant changes to the electronic environment. These include an increasingly hostile online security environment and emerging threats, which do not respect traditional jurisdictional boundaries, and a rapid and ongoing evolution of Australia's information and communications environment, including the forthcoming roll-out of the National Broadband Network.

In response to the changing environment, the Attorney-General and the Minister for Broadband, Communications and the Digital Economy announced in July 2008 a comprehensive review of the Australian Government's e-security arrangements.

The E-Security Review 2008 (the Review) was conducted by a multi-agency team, led by AGD. In accordance with the Review's terms of reference (**Attachment B**), targeted consultation was undertaken with relevant stakeholders and experts in government, business, academia and the community. The consultation process included a call for written submissions and face-to-face meetings. There was significant interest in the Review across all sectors with a large number of submissions received.

The Review examined the Australian Government's e-security policy, programs and capabilities and found that these arrangements work well but require enhancement. The Review made a number of recommendations addressing e-security across government, business and the community on a range of issues including the protection of Australian Government systems, incident response and crisis management, the provision of an adequate legal framework and law enforcement capability, awareness raising amongst home users and small business, and engagement with States and Territories, the commercial Internet industry and international partners.

A key outcome of the Review will be a new Australian Government policy framework for e-security, covering the span of e-security issues across government, business and the community. The new framework will articulate the Australian Government's e-security objectives and identify the strategies and capabilities required to achieve the aim of maintaining a secure and trusted electronic operating environment for both the public and private sectors. The framework will be released later in 2009 and will reflect the totality of the Review's recommendations.

The Review recognised that the provision of an effective legal framework and enforcement capabilities for e-security is a core function and responsibility of government. It is critical that all Australians have access to a robust criminal and civil legal framework that ensures the protection of their identity, privacy and financial information. Key aspects of this activity include a legislative and regulatory framework that is adaptive and flexible, and is monitored on an ongoing basis to ensure it keeps pace with technological and functional changes in the ICT environment. It is essential that such laws are implemented and administered in a manner that maximises outcomes for victims of crime and that law enforcement is given the appropriate tools and powers to ensure this outcome.

The discussion paper prepared for public consultation during the Review, which called for submissions to the Review, specifically asked for input regarding the following issues:

- prevention, investigation and prosecution of cyber crime, and
- legal and law enforcement issues.

Over 70 submissions to the Review were received. While recognising some areas where legal frameworks and law enforcement arrangements could be strengthened, it is important to note that the Review concluded that Australia's existing laws are appropriate, a view supported by submissions to the Review.

The Review recommendations relating to legal and law enforcement issues were in relation to relevant Australian Government agencies working collaboratively to address the following priority issues:

- legal issues associated with the blocking of user access to Internet sites by law enforcement and other agencies
- cross-jurisdictional law enforcement coordination, including with State and Territory police, to better clarify arrangements in regard to crime reporting and escalation protocols for serious e-security incidents, and
- training opportunities and information resources for the legal profession on e-security related issues.

2.4 Coordination and collaboration

2.4.1 Australian Government coordination

2.4.1.1 E-security governance

The Australian Government takes a whole of government approach to combating cyber crime and to e-security more broadly. It coordinates e-security issues through the E-Security Policy and Coordination Committee (ESPaC), chaired by AGD (*refer to terms of reference at* ***Attachment C***).

The ESPaC is an inter-departmental committee that provides whole of government strategic leadership on e-security, determines strategic priorities for the Australian Government, coordinates the response to e-security incidents, and coordinates Australian Government e-security policy internationally.

The structure and operation of the ESPaC was reviewed as part of the 2008 Review. As a result, the ESPaC was restructured to align membership to those agencies that have responsibility for e-security policy, implementation, crisis management and response.

The revised ESPaC is chaired by AGD and its membership is comprised of the following agencies:

- Australian Federal Police (High Tech Crime Operations)
- Australian Government Information Management Office
- Australian Security Intelligence Organisation
- Defence Signals Directorate
- Department of Broadband, Communications and the Digital Economy
- Department of Defence, and
- Department of the Prime Minister and Cabinet.

The Committee meets every second month and out of session as required.

Also as a result of the Review, an implementation and coordination meeting is being established that has a broader membership of agencies across the Australian Government. It is intended that the E-Security Policy and Coordination Committee Implementation and Coordination Meeting (ESPaC-ICM) will support the work of the ESPaC by sharing information on the implementation of Australian Government e-security initiatives. It will also provide a forum for reporting international engagement activities.

2.4.1.2 Joint Operating Arrangements

The Australian Government operational e-security agencies (DSD, AFP and ASIO) have established a set of arrangements called the Joint Operating Arrangements (JOA). The purpose of the JOA is to identify, analyse and respond to threats to, and attacks on, the national information infrastructure. In the event of an incident, the JOA agencies will determine which agency has primary carriage on the basis of the nature of the incident and individual responsibilities. AGD, while not a formal part of the JOA, acts in an advisory and liaison capacity between the JOA and the private sector on matters relating to the protection of systems of national interest.

2.4.1.3 National computer emergency response team

The 2009-10 Budget provided funding for the creation of a national computer emergency response team (national CERT), to be coordinated by AGD.

The new Government-funded national CERT will bring together Australia's existing computer emergency response arrangements, creating a single national point of contact and information resource for e-security information and advice. It will coordinate across government and non-government e-security efforts and will enable all Australians to access information on e-security threats, vulnerabilities in their systems and information on how to better protect their information technology environment.

The new national CERT will incorporate a range of current e-security activities undertaken by Australian Government agencies, such as the Australian Government Computer Emergency Readiness Team (GovCERT.au) in AGD, and provide a contact point for overseas governments to ensure that we keep pace with the e-security environment, internationally and domestically.

The creation of the new national CERT will be done in collaboration with AusCERT, based at the University of Queensland. Transitional arrangements will begin in July 2009 with the new Australian Government national CERT operational by June 2010.

The national CERT will complement the Cyber Security Operation Centre, within the Department of Defence (*refer to Section 2.4.1.4 below*).

The new national CERT arrangements and other initiatives arising from the recent Review will significantly enhance and improve the capacity of business, Government and the community to respond to and recover from cyber security incidents.

2.4.1.4 Cyber Security Operations Centre

The establishment of a Cyber Security Operation Centre (CSOC) was announced as part of the *Defence White Paper 2009 – Defending Australia in the Asia Pacific Century: Force 2030*. The CSOC will provide the Australian Government with better cyber situational awareness, coordinate responses to e-security incidents of national importance and will maintain a 24x7 watch on cyber activities which might threaten Australia's national security.

The CSOC will also provide information to the national CERT that can be packaged into products for consumption by business. It will include staff from relevant agencies including the Department of Defence, ASIO, AFP, and from AGD's GovCERT.au/national CERT.

2.4.1.5 Australian Government systems

As the national authority on the security of ICT across government, DSD provides a range of information security services to ensure that sensitive government electronic information systems are not susceptible to unauthorised access, compromise or disruption. AGIMO also works with Australian Government agencies in managing their ICT, including through the provision of high-level strategic advice on the technology-enabled transformation of government services and administration for the Australian Government.

The Review examined issues in relation to enhancing the resilience and integrity of Australian Government online systems that are used by the public. The move to provide more government services online is common around the world and has provided greater levels of access to information, improved efficiency and convenience. Whilst recognising the need for users to take responsibility in securing their own systems and information, the Review examined what guidance can be given to Australian Government agencies on issues to consider when transacting with the public so as to minimise exposing clients to additional risk. Issues to consider include the security of personal data being transmitted over the Internet during a transaction, and the security of any personal data stored on the client's system as a result of the transaction.

2.4.2 *Cross jurisdictional collaboration*

The growing trend of interconnection between Commonwealth and State and Territory systems makes it increasingly important for the Commonwealth to engage with States and Territories on e-security. The Commonwealth is currently looking to strengthen its relationship with the States and Territories on e-security issues.

The Review found that engaging with State and Territory governments in a dialogue on e-security issues will allow the Commonwealth to raise the profile of its e-security activities and facilitate information sharing on e-security risk, threats and risk mitigation. As a result of the Review, AGD is investigating whether it is possible to utilise existing cross-jurisdictional forums, such as the Cross Jurisdictional Chief Information Officers' Committee, to more formally engage with the jurisdictions on e-security issues.

The Australian Government currently does not have formal programs for engaging with local government on e-security. The formalisation of communication between the Commonwealth and State and Territory governments on e-security may provide a pathway to reach out to local governments on this issue in the future.

2.4.3 *Business-government partnership*

Australia's national security, economic prosperity and social well-being is dependent on the physical facilities, supply chains, information technologies and communication networks that make up Australia's critical infrastructure. Business, government and the Australian public require reliable access to the essential goods and services that critical infrastructure provides.

Critical infrastructure in Australia is both privately and publicly owned and operated, although substantial aspects of it are privately owned. Owners and operators of critical infrastructure have the primary responsibility for securing their assets, ensuring continuity of services and are also best placed to manage risk to their operations. However, individual companies may not have the information about all threats and vulnerabilities, or the resources to assess or mitigate the risks from a whole-of-sector perspective. The Australian Government does not take a regulatory approach to critical infrastructure protection, preferring instead to work with and support business in an environment that promotes information exchange and best practice.

To meaningfully engage with these critical infrastructure and key businesses, an environment of cooperative trust is needed between government and business, and ideally between business and business. The Australian Government has established a range of initiatives to facilitate a business-government partnership for e-security and critical infrastructure protection which are detailed in the sub-sections below. However, it is noted that the new national CERT arrangements (*refer to section 2.4.1.3 above*), once operational, will subsume some of these arrangements (eg GovCERT.au).

2.4.3.1 *Trusted Information Sharing Network for Critical Infrastructure Protection (TISN)*

Established in 2003 in recognition of the importance of Australia's critical infrastructure, the TISN is a forum where industry and government can share vital security-related information on critical infrastructure protection and organisational resilience. The TISN has maintained an all hazards mandate that seeks to address generic threats to, and vulnerabilities in, critical infrastructure, and measures and strategies to mitigate risk.

The TISN includes nine infrastructure sector groups covering banking and finance, communications, emergency services, energy, food chain, health, mass gatherings, transport and water. Of particular relevance in the context of cyber crime and e-security is the Communications Sector Infrastructure Assurance Advisory Group, which brings together owners and operators of Australia's critical infrastructure in the communications, international submarine cables, postal and broadcasting sectors with the aim of enhancing the resilience of the sector. It is this infrastructure that is utilised as the delivery mechanism for cyber crime and related activities.

The value of a business-government partnership through the TISN was demonstrated by the success of the inaugural All Sectors TISN Forum held in May 2008. The Forum brought together representatives from across the nine industry sectors represented in the TISN to share information on the activities of the sector groups, consider future trends and discuss the strategic direction of the TISN.

2.4.3.2 Information exchanges

The Australian Government Computer Emergency Readiness Team (GovCERT.au), within AGD, works with the owners and operators of critical infrastructure and key business to provide them with situational awareness of e-security threats.

Building on the success of the TISN, and as a result of the Review, GovCERT.au has established three information exchanges to enable the sharing of detailed technical information between government and business. E-security information exchanges have been established with the banking and finance sector, the communications sector and owners and operators of control systems in power and water utilities. The information exchanges enable a two-way exchange of sensitive e-security technical information between the Australian Government and Australian owners and operators of critical infrastructure and key business in a highly trusted environment.

They will also encourage and facilitate the sharing of security-related information between companies. The information exchanges will enhance the ability of both government and business to understand the threats and vulnerabilities we face and provides the private sector with information that will assist them to more quickly respond to cyber incidents.

2.4.3.3 E-security exercise program

To improve the ability of governments and critical infrastructure owners and operators to manage e-security incidents, AGD was tasked, as an outcome of the 2006 review, to develop a cyber exercise program. As a result, the Australian Government's cyber exercise program consists of discussion exercises for high level committees, international drill exercises, and a national exercise held in conjunction with an international cyber exercise, 'Cyber Storm', every two years. Exercises test Australia's level of readiness for a major e-security incident and allow government agencies and private sector organisations to test and validate their e-security incident response and communication mechanisms. They are also a means to further explore interdependencies with other infrastructure providers. AGD is currently reviewing the e-security crisis arrangements and, as roles and responsibilities are clarified, elements will be added to the exercise program.

The bi-annual international Cyber Storm exercise (led by the United States Department of Homeland Security) provides a framework for a comprehensive national exercise involving the Australian Government, other jurisdictions, the private sector and not-for-profit agencies. Cyber Storm II was conducted in March 2008 and was structured and executed as a large-scale national exercise within an international framework. Canada, New Zealand, the United Kingdom and the United States were also participants. Australia's participation was second only to the United States, and involved Australian Government agencies, State and Territory governments and the largest contingent of private sector organisations ever involved in an Australian Government-sponsored exercise. The exercise structure allowed participants to exercise their internal incident response and communications in a national framework that allowed external communications to be more than notional and which encouraged a collaborative response.

Planning for Cyber Storm III, to be held in late 2010, has commenced. Most Australian participants, both government and non-government, in Cyber Storm II have indicated that they are interested in participating in Cyber Storm III.

Exercises such as Cyber Storm are critical in maintaining and strengthening cross-sector, inter-governmental and international relationships, enhancing processes and communications linkages, as well as ensuring continued improvement to e-security procedures and processes.

2.4.4 Home user engagement

More than 15.3 million Australians are using the Internet to access a range of services and applications. However many of these home and small business users are highly vulnerable to electronic threats due to their lack of skills or through not undertaking the necessary precautions to protect themselves online. The Australian Government, through DBCDE, provides a range of awareness raising and education initiatives to improve the e-security of home users and small businesses. DBCDE will outline their initiatives in these areas in their submission to the Inquiry.

Recognising the unique role Internet service providers (ISPs) can play in helping to educate, inform, influence and protect Australian Internet users, the Review recommended the development of a code of practice for ISPs. DBCDE and ACMA have responsibility for this recommendation, and this issue will also be addressed in DBCDE's submission.

2.4.5 International engagement

Due to the borderless nature of the online environment, continued international collaboration, coordination and cooperation is critical in securing the online environment. The Australian Government recognised in the Review the multi-jurisdictional nature of Internet-based threats. The Government is working collaboratively with like-minded governments both bilaterally and in multilateral fora to develop longer term solutions to Internet threats as well as to promote e-security awareness, marshal expertise, and eliminate safe havens for cyber criminals. One of the challenges internationally is that criminals can easily locate and relocate their operations in jurisdictions where their activities are not illegal, the legal penalties are lower or where law enforcement lacks the capability to adequately undertake technologically sophisticated investigations. If the problem is fixed in a particular jurisdiction, the criminals will very rapidly move to another jurisdiction and the problem continues.

The actions of other governments, businesses and consumers overseas have an e-security impact on Australian Internet users and vice versa. National policies, capabilities and programs in isolation can never be fully effective in dealing with e-security issues. International engagement provides Australia the opportunity to influence outcomes that have the potential to positively or negatively impact upon the e-security of government systems, systems of national interest, business and home users.

2.4.5.1 E-security engagement

The Australian Government currently engages formally with the international community on e-security issues through a range of fora, including the:

- **International Watch and Warning Network (IWWN)** is an international forum for international cooperation and coordination on cyber information sharing and incident response. It is comprised of government cyber security policy makers, managers of computer security incident response teams with national responsibility and law enforcement representatives with responsibility for cyber crime matters.
- **Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL)** aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing and implementing appropriate telecommunications and information policies.
- **Meridian** process brings together senior government officials from around the world who are policy makers on issues of critical information infrastructure protection (CIIP).
- **International Telecommunication Union (ITU)** is the leading United Nations agency for information and communication technologies and is currently undertaking a range of e-security issues under its Global Cybersecurity Agenda. The ITU's powers can bind member countries to take specific courses of action.
- **OECD Working Party for Information Security and Privacy (WPISP)** provides a platform for pursuing international aspects of Australian communications policy relating to cyber security, critical infrastructure protection, authentication, privacy, malware and spam.
- **International Multilateral Partnership against Cyber Threats (IMPACT)** is a public-private initiative against cyber-terrorism led by Malaysia. It is the first global public-private initiative against cyber-terrorism and brings together governments, industry leaders and e-security experts.
- **Forum of Incident Response and Security Teams (FIRST)** conference brings together a variety of computer security incident response teams from government, commercial, and educational organisations. It aims to foster cooperation and coordination in incident prevention to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. There is also an associated meeting of national computer emergency response teams (CERTs) known as SECOND that provides a mechanism for cooperation and collaboration to solve many of the issues that national CERTs share in common.

The Australian Government has also developed less formal bilateral and multilateral partnerships with a number of key allies to coordinate and collaborate on policy and operational issues as well as in the development of international cyber exercises. These are in addition to relationships Australian Government agencies have with counterpart agencies internationally on specific subject matter areas, such as the AFP's participation in the Cybercrime Working Group (CCWG).

The strong relationships Australia has with regional partners and key allies on e-security issues are strongly supported by joint critical infrastructure protection partnership arrangements focused on e-security matters.

2.4.5.2 Council of Europe Convention on Cybercrime

There are a number of general criminal-related conventions internationally; however the key one is the *Council of Europe Convention on Cybercrime (2001)*, which is the only multilateral treaty in force that specifically addresses cyber crime.

The Convention opened for signature on 23 November 2001, and entered into force on 1 July 2004. Since then, 20 State Parties have signed the Convention, and another 26 States have ratified or acceded to it, including the United States. The Convention requires State Parties to criminalise a range of conduct relating to cyber crime, and to provide the procedural law and law enforcement powers necessary to investigate and prosecute cyber crime offences. The Convention aims to establish a fast and effective regime for international cooperation in responding to cyber threats such as malware, online fraud, botnets that can attack critical infrastructures, and the use of the Internet to sexually exploit children.

Australia is not currently a party to the Convention. However Australia is already compliant with some obligations contained in the Convention due to the existence of a range of cyber crime offences and enhanced powers for investigating cyber crime. There remain a number of complex issues that the Government will need to consider, some of which may require significant legislative amendment.

The Australian Government is currently reviewing existing domestic legislation to identify what action may be necessary to implement the Convention in Australia's domestic law, should it decide to become a party to the Convention.

2.5 Related areas of Australian Government policy

Policy relating to e-security and cyber crime issues intersects and overlaps with a number of other areas of government activity. These include cybersafety, privacy, consumer fraud, identity security and telecommunications interception. The first three issues are the responsibility of other Australian Government agencies; the latter two fall within the remit of AGD responsibility and therefore an overview of these areas is provided below.

2.5.1 Identity security

2.5.1.1 Background

Australia's system of identity management comprises a dispersed network of documents, cards and other credentials issued by both government and private sector organisations. A significant drawback of federated systems of identity is the potential for the *fragmenting* of an individual's identity, which can occur when a person enrols for services or goods using different name/s or other personal details.

It is not suggested that an individual deliberately chooses to use different name/s or other details with an intention to deceive; although this is no doubt the case in some cases. As Australians have a common law right to a change of name through usage or repute, individuals are usually able to exercise wide discretion to choose to use different name/s to support different aspects of their lives. A preferred name may be based on any number of individual preferences, including a derivative of a name (eg 'Liz' rather than 'Elizabeth'), use of a middle name, nickname, or pseudonym. A person from a non-English speaking background may adopt an Anglicised name for use as part of their social identity. The same person may have multiple on-line identities; each tailored to a specific context. A name used in a chat room may be different to that used to buy goods on-line.

In certain circumstances, however, individuals have limited options to use a preferred name or to be anonymous. For example, to apply for a government-issued passport, or a bank-issued credit card, a person must use name/s that establish their legal identity, and provide proof of identity (POI) documents to verify their claimed identity. POI documents provide documentary evidence of a person's full name that is linked to their legal identity. Each Australian has only one legal identity at a time. As such, while Australians are legally entitled to use a *preferred* name at any time, and may choose to use different preferred names in various contexts, a formal process is required to alter name/s linked to a person's legal identity.

There is wide variation among agencies in the extent to which the name linked to a person's legal identity is verified using documentary evidence. Many government-issued documents, cards and other credentials, which are used in the community to verify a person's identity, were not issued, and were never intended, to be used for identity verification purposes. While policy and procedures regulating the collection and amendment of personal information may have been strengthened in recent years, agency data holdings accumulated over many years, sometimes decades, are known to be of variable quality and accuracy.

2.5.1.2 Identity crime

In the past decade, there has been increasing awareness of the dangers posed by identity crime. The costs to individuals and business from identity crime are significant and rising, with the Australian Bureau of Statistics estimating that personal frauds of various kinds cost nearly $1 billion a year, and that half a million Australians have experienced at least one form of identity fraud. Preventing identity crime is also important to reduce the threat of terrorist and other serious criminal activity, which is often founded on the use of false or multiple identities.

Recognition of the threats posed by identity crime has led to a number of measures directed at preventing online identity crime through systematic and whole of government improvements to the national identity management system. The centrepiece of this response is the National Identity Security Strategy (NISS), which was endorsed by the Council of Australian Governments (COAG) in 2005. The Strategy is a cross-jurisdictional, whole of government approach that has six elements including:

- developing a national document verification service to combat the misuse of false and stolen identities
- improving standards and procedures for enrolment and registration for the issue of POI documents
- enhancing the security features on POI documents to reduce the risk of incidence of forgery
- improving the accuracy of personal identity information held on organisations' databases
- enabling greater confidence in the authentication of individuals using online services, and
- enhancing the national interoperability of biometric identity security measures.

These measures are intended to make it more difficult for criminals to create new identities or incorporate fabricated or inaccurate information into false identification credentials.

2.5.1.3 Future initiatives

Work is continuing to improve the integrity of key identity credentials. This work is essential to prevent threats that exist in the current paper-based identity system, and to prevent current vulnerabilities being transferred in the future to digital identity credentials.

Identity security strategies are being developed that are oriented towards the digital world, which recognise identity management as an enabler of the delivery of services and benefits, as well as a shield against both internal and external threats. A number of key government priorities are dependent on securing the digital integrity of key identity credentials, including growing the e-economy, more efficient delivery of service/s, and greater access to secure business-to-government transactions.

The digital world is characterised by the speed with which both opportunities and threats emerge, and a shift from face-to-face to online transactions. This means that identity management systems are becoming more interconnected and inter-reliant. The OECD has recognised the need for a coordinated approach to identity management, and these developments are being closely monitored in Australia[1].

Biometrics offer the potential to establish a unique identity record, by linking personal information (such as a person's name and address) with an individual's biometric (such as facial image or fingerprints). Developing reliable, consistent and nationally interoperable biometric applications are essential to establish trust and confidence in the security of on-line transactions and expand the Internet and the digital economy.

2.5.2 Telecommunications interception

AGD is responsible for the administration of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). It is noted that conduct that may constitute a cyber crime offence may also be in breach of this Act.

The TIA Act makes it an offence for a person to intercept a communication during its passage over a telecommunications system, without knowledge of the person(s) making the communication. There are a number of exceptions from this prohibition, the most important of which is the ability to intercept communications under a warrant.

The TIA Act provides for the lawful interception of and access to communications to assist in the investigation of serious offences. A serious offence includes a number of telecommunications offences in the Criminal Code such as using a carriage service for possessing, controlling, or supplying child pornography. Serious offences for the purposes of the TIA Act also include cyber crime offences that breach Part 10.7 of the Criminal Code which include the unauthorised access, modification or impairment of a computer. Accordingly, the TIA Act provides law enforcement agencies with a mechanism to investigate and prosecute such offences in a manner that allows them to access real time or near real time information.

The TIA Act also regulates access to stored communications. Stored communications are communications that either have ceased, or have not commenced, passing over a telecommunications system, and are accessed on equipment operated by a carrier. The TIA Act makes it an offence for a person to access a stored communication without the knowledge of the

[1] See http://www.oecd.org/dataoecd/55/48/43091476.pdf

sender or the intended recipient of the communication. There are also exceptions from this prohibition, and again the most important one is the ability to access stored communications under a warrant.

Attachment A

SUMMARY OF RELEVANT OFFENCES IN THE CRIMINAL CODE

Part 10.6

Part 10.6 of the *Criminal Code Act 1995* (Cth) (Criminal Code) contains offences which criminalise the misuse of telecommunications, such as the Internet. The key offences relating to online bullying and harassment include:

- Section 474.14 – *Using a telecommunications network with intention to commit a serious offence* – This offence is intended to be broad and cover the use of the Internet or another telecommunications network to commit serious offences, for example fraud or stalking. A serious offence is a Commonwealth, State or Territory offence with a maximum penalty of five or more years imprisonment. This offence is punishable by the maximum penalty of the serious offence.
- Section 474.15 – *Using a carriage service to make a threat* – This offence is intended to cover threats to kill or cause serious harm that are made over the Internet. A threat to kill is punishable by a maximum penalty of 10 years imprisonment. A threat to cause serious harm is punishable by a maximum penalty of seven years imprisonment.
- Section 474.17 – *Using a carriage service to menace, harass or cause offence* – This offence is intended to cover online conduct that a reasonable person would find to be menacing, harassing or causing offence. This is a broad offence that covers a wide range of conduct. There is no definition in the Criminal Code for the terms ‘menace’ or ‘harass’. This offence is punishable by a maximum penalty of three years imprisonment.
- Sections 474.19 – *Using a carriage service for child pornography material*, Section 474.20 – *Possessing, controlling, producing, supplying or obtaining child pornography for use through a carriage service*, Section 474.22 – *Using a carriage service for child abuse material*, Section 474.23 – *Possessing, controlling, producing, supplying or obtaining child abuse material for use through a carriage service* – These offences are intended to cover the use, access, distribution, production, supply and distribution of child pornography or child abuse material online. These offences are punishable by a maximum penalty of 10 years imprisonment.

Part 10.7

Part 10.7 of the Criminal Code contains offences which criminalise the misuse of computers. The penalties for these offences range from two to 10 years. A summary of the offences in part 10.7 is as follows:

- Section 477.1 – *Unauthorised access, modification or impairment with intent to commit a serious offence* – This offence is intended to cover unauthorised use of computer technology to commit serious crimes, such as fraud or terrorist offences. A serious offence is a Commonwealth, State or Territory offence with a maximum penalty of five or more years imprisonment.
- Section 477.2 – *Unauthorised modification of data to cause impairment* – This offence is intended to cover the unauthorised modification of data on a computer that would impair access to, or the reliability, security or operation of the data. For example, a person who uses the Internet to infect a computer with malware. To fall with in Commonwealth jurisdiction, the offence needs to have occurred over a carriage service or involve a Commonwealth computer or data. This offence is punishable by a maximum penalty of 10 years imprisonment.

- Section 477.3 – *Unauthorised impairment of electronic communication* – This offence is intended to cover cyber-attacks such as denial of service attacks, where a server is inundated with a large volume of data, which is intended to impede or prevent its functioning. This offence is punishable by a maximum penalty of 10 years imprisonment.
- Section 478.1 – *Unauthorised access to, or modification of, restricted data* – This offence is intended to cover unauthorised access to or modification of data held on a computer which is restricted by an access control system. For example, hacking into password protected data. This offence is punishable by a maximum penalty of two years imprisonment.
- Section 478.2 – *Unauthorised impairment of data held on a computer disk* – This offence is intended to cover the unauthorised impairment of data held on a computer disk, credit card or other device used to store data by electronic means. For example, impairment of data by passing a magnet over a credit card. This offence is punishable by a maximum penalty of two years imprisonment.
- Section 478.3 – *Possession or control of data with intent to commit a computer offence* – This offence is intended to cover people who possess programs designed to hack into other people's computer systems or impair data or electronic communications. For example, possessing a program which will enable the offender to launch a denial of service attack against a Commonwealth Department's computer system. This offence is punishable by a maximum penalty of three years imprisonment.
- Section 478.4 – *Producing, supplying or obtaining data with intent to commit a computer offence* – This offence is intended to cover the production and/or supply of data to be used in a computer offence. This offence is punishable by a maximum penalty of three years imprisonment.

Investigative powers under the Crimes Act

Part IAA of the *Crimes Act 1914* contains provisions which allow law enforcement officer to search and seize electronic data. These provisions also enable law enforcement officer to seek an order from a magistrate to require a person to provide a password or other means of accessing encrypted data. Law enforcement may also use electronic devices found during the search of a premises to access data which is stored off site.

Part IAB allows law enforcement to commit criminal offences as part of a controlled operation to investigate the above offences with a maximum penalty of three or more years. Part IAC allows law enforcement officers to use a false identity to investigate all of the above offences.

Attachment B

E-SECURITY REVIEW 2008

TERMS OF REFERENCE

The Attorney-General's Department is to lead a review of the Australian Government's e-security policy, programs and capabilities, assisted by other agencies represented on the E-Security Policy and Coordination Committee. The review will take account of both the threat from electronic intrusions into Australian networks and the threat from complementary attacks on their physical, administrative or personnel security arrangements.

The purpose of the review is to develop a new Australian Government E-Security Framework in order to create a secure and trusted electronic operating environment for both the public and private sectors.

The review will:

1. develop a new Australian Government policy framework for e-security, covering the span of e-security issues across government, business and the community
2. examine current programs, arrangements and agency capabilities and capacities that contribute to e-security, including:
   a) those being implemented by agencies under the E-Security National Agenda
   b) incident response and crisis management arrangements for e-security, including the recommendations from Australia's participation in Exercise Cyber Storm II, and
   c) other relevant information and communications technologies (ICT) initiatives being undertaken by the Commonwealth and by State and Territory governments

   to establish their suitability and effectiveness to achieve the policy objectives of the new Framework.
3. address emerging e-security issues including:
   a) those resulting from technological change, including roll-out of the National Broadband Network, and
   b) an increasingly hostile online security environment, which does not respect traditional jurisdictional boundaries
4. consider opportunities provided by international cooperation, including engagement with similar economies and like-minded governments
5. bring forward recommendations, prioritised in accordance with an assessment of risk, for consideration by Government to:
   a) tailor programs and agency capabilities and capacity to achieve the policy objectives of the new Framework
   b) address current and emerging threats, and
   c) determine how to measure the success of each approach
6. principally focus on measures to be effective in the period to mid-2011, but also take into account longer term considerations, and
7. consult with relevant stakeholders and experts in government, business, academia and the community.

The review is to be completed for Government consideration by October 2008.

An executive committee comprising senior representatives of the Attorney-General’s Department, the Defence Signals Directorate, ASIO, the Department of the Prime Minister and Cabinet, the Department of Broadband, Communications and the Digital Economy, the Australian Federal Police and the Australian Government Information Management Office will provide oversight of the Review.

Attachment C

E-Security Policy and Coordination Committee (ESPaC)

TERMS OF REFERENCE

Role

1. The ESPaC is the inter-departmental committee that coordinates the development of e-security policy for the Australian Government. The ESPaC will:

- provide whole-of-government strategic leadership on e-security
- determine priorities for the Australian Government
- coordinate the response to e-security incidents, noting that its coordination and policy functions do not extend to the oversight of operations
- coordinate Australian Government e-security policy internationally, and
- be supported by the ESPaC Implementation and Coordination Meeting (ESPaC-ICM).

The national security agencies may meet separately to discuss operational matters, and/or matters where ‘need-to-know’ principles apply.

Function

2. The ESPaC will:

- monitor the effectiveness of e-security arrangements and advise Government on the implementation of e-security measures
- coordinate the risk-based development of e-security policy
- oversee and coordinate e-security crisis management arrangements consistent with the broader national crisis management arrangements
- exercise incident response readiness, both domestically and internationally
- promote the maintenance of relationships with public and private organisations involved in e-security issues
- promote awareness raising and behaviour changing initiatives
- maintain an annual work plan
- cooperate with and assist the Protective Security Policy Committee in the development of Australian Government protective security policy, and
- oversee and direct the activities of the ESPaC-ICM.

Accountability

3. The ESPaC will formally report the progress of its annual work plan to the Deputy National Security Advisor (DNSA) on an annual basis.

4. Other e-security issues that require higher level policy consideration may be referred to the Homeland and Border Security Policy Co-ordination Group (HPCG) on an ‘as needs’ basis.

5. The ESPaC will also coordinate the provision of an assessment of the threat and security environment to the National Security Committee of Cabinet, through the Secretaries' Committee on National Security, as required.

Membership

Membership list

6. The ESPaC will comprise representation from those Australian Government agencies that have responsibility for e-security policy, implementation, crisis management and response, namely:

- Attorney-General's Department (Chair)
- Australian Federal Police (High Tech Crime Operations)
- Australian Security Intelligence Organisation
- Defence Signals Directorate
- Department of Broadband, Communications and the Digital Economy
- Department of Defence
- Department of Finance and Deregulation – Australian Government Information Management Office, and
- Department of the Prime Minister and Cabinet.

Additional agencies, organisations and/or representatives of other committees may be invited by the Chair to attend specific meetings or to otherwise contribute to the ESPaC as required.

Principles of membership

7. To enable appropriate representation and perspectives of agencies, agency representation on the ESPaC will comprise up to two representatives, led by a Senior Executive Service (SES) officer, with the expectation that the ESPaC member will be authorised to make commitments on behalf of their agency.
8. ESPaC attendees shall have a minimum SECRET national security clearance.

Role of ESPAC-ICM in support of ESPaC

9. The ESPaC will be supported in its coordination and policy development role by the ESPaC-Implementation and Coordination Meeting (ICM), which has a broader membership base and includes additional agencies with an interest in e-security issues. The ESPaC may task the ESPaC-ICM with specific projects as required.

Administrative arrangements

Relationships with other committees

10. The ESPaC will develop and maintain linkages with the Chief Information Officer Committee (CIOC) and the Protective Security Policy Committee (PSPC) and will promote greater linkages between computer security officers in Australian Government agencies.

Chair and secretariat

11. The ESPaC will be chaired by the First Assistant Secretary, National Security Resilience Policy Division, Attorney-General's Department.

12. The Attorney-General's Department will provide secretariat support to the ESPaC.

Frequency of meetings

13. The ESPaC will meet at 9.30am on the first Tuesday of every second month (even numbered months), or as required, in an appropriately secure venue.

Extraordinary ESPAC

14. The ESPaC has a role in crisis management arrangements and may be called out of session in this role by or in consultation with the Chair.

Agenda structure

15. The agenda will be split into items for noting, discussion, and decision. Items for noting will only be discussed by exception.

Timelines

19 working days prior to meeting	Secretariat calls for agenda topics with draft agenda
17 working days prior to meeting	Members to provide proposed agenda items
15 working days prior to meeting	Agenda finalised
10 working days prior to meeting	Agenda papers to be provided to the Secretariat
8 working days prior to meeting	Secretariat to circulate final agenda and papers to members
3 working days prior to meeting	Members to advise Secretariat of attendance
Meeting	
7 - 9 working days post meeting	Draft summary record and action items circulated
Between Meetings	Out of session work may progress between meetings and reports may be provided to members for consideration

Secretariat contact details

16. The ESPaC Secretariat can be contacted on:

Tel 02 6141 2974 (or 02 6141 2960)
Fax 02 6141 3046
Email espac@ag.gov.au