Government Response

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

Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime

The Government welcomes the report of the House of Representatives Standing Committee on Communications, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime.*

The Committee's report makes clear that cyber space is an increasingly challenging policy area for government. The internet is now an integral part of Australians' everyday lives. Business and banking are increasingly being conducted online. The digital economy is essential to Australia's productivity, global competitive standing and improved social well-being. With the massive uptake of social networking in recent years, Australians are now sharing more personal information online with friends, family and the broader community. The breadth of issues considered by the Committee demonstrates the challenges posed by the central role of the internet and information and communication technology in Australians' everyday lives. While the internet offers many benefits, there are also a range of safety and security risks associated with its use. It is imperative that governments, industry and individuals take action to mitigate these risks.

The role for government

As outlined in the submissions from government departments and agencies, considerable work is being done on cyber crime issues. However, due to the pace of technological change and social trends, there is an ongoing requirement for government to review and adapt its response to ensure that it remains as effective as possible.

It is evident that current efforts in this area by government, industry and community organisations need to be more coordinated and strategic. The Committee's report envisages a key role for the Commonwealth Government in addressing these issues through assuming a greater coordinating role. The new position of Cyber Policy Coordinator (CPC) within the Department of the Prime Minister and Cabinet (PMC) will provide a single point of policy coordination for issues across the cyber spectrum. This spectrum spans a number of separate but closely interconnected spheres, which can be broadly described as:

- online consumer protection – promoting fair trade, protecting consumer rights and preventing and responding to online scams
- cyber safety – protecting children from harmful online content, inappropriate contact and bullying/harassment
- cyber crime – preventing, detecting and prosecuting crimes directed at computing and communications technologies and crimes where the use of

computing or communications technologies is integral to the commission of the offence

- cyber security – ensuring the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means, and

- cyber operations – protecting Australia's national security interests in cyber space.

The Committee also observed that there is the need for a concept of shared responsibility for personal internet security, with a role for individuals, industry and government. The Government shares this view, which is reflected in the Government's *Cyber Security Strategy*. It is important for industry, government, law enforcement and non-government organisations to work cooperatively and develop strategies to combat online criminal activity.

The role for government in relation to cyber crime is broad, spanning regulation, enforcement, education and awareness raising, international engagement, and consultation with industry and individuals. While the Government is working in many areas to ensure that Australians' online experience is as safe as possible, it cannot provide complete protection from all online risks. Ultimately, businesses and individuals must take responsibility for their own safety and security online. This means being aware of the potential risks and taking the necessary steps to protect themselves. Business must develop safe practices to protect both themselves and their customers, and promptly report incidents when they occur. Individuals must ensure that they take appropriate measures to protect themselves online including installing appropriate security software and keeping it up to date, and adopting secure online practices and behaviours.

Current work on cyber crime

Since the Committee concluded its inquiry, the Government has taken further steps to address cyber crime. A number of the Committee's recommendations have already been acted upon.

The Commonwealth is working closely with state and territory governments to adopt a more coordinated national approach to combating cyber crime between and across jurisdictions. A National Cyber Crime Working Group (NCWG) has been established under the auspices of the Standing Committee of Attorneys-General (SCAG) to review existing arrangements aimed at combating cyber crime and provide advice on how they could be improved. This will include recommendations for clarifying lines of responsibility and enhancing coordination between law enforcement agencies.

Recognising that there are a range of existing mechanisms used to report cyber crime, one of the issues currently being examined by the NCWG is mechanisms to improve the reporting of online offences, including through the possible establishment of a central online reporting facility. The Committee's consideration of this issue in its report is a useful input for the NCWG's deliberations.

Commonwealth, State and Territory Governments are also reviewing the model computer offences developed in 2001 to ensure they remain effective in light of technological advances and other key trends.

The Government continues to progress its vision for a secure, resilient and trusted cyber environment through the *Cyber Security Strategy*. The Strategy outlines how the Government is harnessing a comprehensive range of measures to help protect government, business and individual Australians. It also highlights the importance of individual users being vigilant and informed about online threats.

The Australian Federal Police (AFP) High Tech Crime Operations (HTCO) portfolio continues to provide the AFP with an enhanced capability to combat technology enabled crime and to facilitate centrally-coordinated high technology operations support. The HTCO prevents, detects, investigates and prosecutes technology crime across all areas of AFP policing.

International cooperation

The Government recognises that the global nature of cyber crime means that agencies in Australia and around the world must collaborate to target those who seek to exploit the internet for criminal gains. Implementing consistent legislation and strategies is essential in ensuring that cyber criminals are not able to find safe haven in some jurisdictions at the expense of others. Effective arrangements for law enforcement to access data held overseas will also be important. This need for a shared international approach is why the Government announced Australia's intention to accede to the Council of Europe Convention on Cybercrime on 30 April 2010. The Convention is the only binding international treaty on cyber crime and aims to establish a common criminal policy to protect society against cybercrime by adopting appropriate legislation and fostering international cooperation. It focuses on having a 24/7 capability to identify internet crimes and work with other nations to prosecute those crimes.

Australia is currently in a good position to comply with the majority of obligations under the Convention. Some amendments to domestic laws will be required to ensure Australia can meet the information sharing and international cooperation requirements. The Government is moving expeditiously to ensure that Australia is in a position to accede to the Convention.

In addition to this the Government is involved in a range of international collaborative activities to combat cyber crime. One such example is the Australian Communication and Media Authority's (ACMA's) participation in the London Action Plan (LAP). The LAP is the preeminent international collaboration on anti-spam and fosters links between international law enforcement authorities.

The national computer emergency response team (CERT Australia) is actively engaging with other CERTs internationally, and led Australia's participation in the multinational Cyber Storm III exercise. CERT Australia has recently accepted an invitation to join the Asia-Pacific CERT community, and is negotiating bilateral cooperative agreements with a range of countries in the region.

The Government also actively engages with international organisations to address online safety issues. For example, the ACMA is a member of INHOPE, the International Association of Internet Hotlines which supports hotlines all over the world to respond in collaboration with law enforcement agencies to reports of child abuse content.

Education and awareness raising

In May 2008, the Government dedicated $125.8 million over four years to a cyber-safety plan which includes initiatives to inform and educate parents and children about the risks of internet use and to provide internet safety advice, tools and online help. The ACMA's Outreach program targets teachers, children and their parents through internet safety awareness presentations. The ACMA has also launched a Cybersmart website (www.cybersmart.gov.au), providing free access to internet safety and security advice as well as to an extensive range of teaching resources. The site includes referral mechanisms to an online helpline, which offers free, confidential advice and support to children when dealing with issues such as cyber-bullying.

The Government has also developed a Cybersafety Help Button which is an online resource that gives children easy access to cyber safety assistance and information. The button will be freely available to the Australian public and downloadable onto personal computers.

In addition, the Government is also developing an Easy Guide for Social Networking Sites which will provide accessible information outlining the key cyber safety features available on many of the popular social networking sites. The guides are designed to inform young people and their parents to assist them in choosing sites in which to participate.

The Government's efforts to educate the community about how to be both secure and safe online were showcased during the 2010 Cyber Security Awareness Week. This involved more than 150 industry, community and consumer groups and state and territory governments around Australia, both in metropolitan and regional areas. As part of this, the Government launched the *Protecting Yourself Online – What Everyone Needs to Know* booklet. Government agencies with an interest in cyber security were involved in the production of the booklet, resulting in a 'one-stop shop' for all information relevant to Australia's cyber environment that complements the Government's other public awareness raising activities.

The 2010 Cyber Security Awareness Week also saw the launch of a voluntary cyber security code of practice for internet service providers (ISPs) (the ISP Code). Developed by the Internet Industry Association (IIA) in partnership with the Government, the ISP Code provides a consistent approach to help ISPs inform, educate and protect their customers in relation to cyber security issues. The ISP Code encourages ISPs to monitor their networks for malicious 'botnet' activity, including through subscribing to the ACMA's Australian Internet Security Initiative (AISI), to notify their customers should their computers become compromised and to assist their customers in remediating their compromised computers.

The ISP Code complements the Stay Smart Online website (www.staysmartonline.gov.au), through which the Government makes available information and advice for Australian internet users on the simple yet effective steps they can take to protect themselves online. This website features a range of free resources including an interactive, self learning education package, also known as budd:e, for students in primary and secondary school and a plain language alert service which provides information on the latest cyber security threats and vulnerabilities and how to address them.

The cyber safety program 'ThinkUKnow' is a joint partnership between the AFP and Microsoft Australia and sponsored by ninemsn to deliver interactive presentations to parents, carers and teachers through primary and secondary schools to raise awareness of issues facing youth online.

Partnering with Business

The Government is also committed to partnering with business on cyber security and this work is led by CERT Australia. CERT Australia provides business with information and advice on the latest threats and vulnerabilities and acts as the national coordination point with the private sector and other international CERTs in the event of a major cyber security incident. Through its work with the private sector, CERT Australia aims to ensure that the systems managed by businesses to provide everyday services for Australians are safe and secure. In this way, CERT Australia works to improve the cyber security and resilience not just of our critical infrastructure but also of Australia's broader digital economy.

Strong laws and effective, well-resourced law enforcement agencies remain critical to the fight against cyber crime. However, the nature of the internet, including its global reach, the anonymity it affords and the sheer speed and amount of data traversing it every second means that there continue to be practical limitations on the ability of any country's law enforcement agencies to investigate and prosecute cyber criminals. While the Government will continue to ensure Australia has a strong legal and law enforcement framework in place to combat cyber crime, it will also seek to employ a broader range of market-based approaches in encouraging the adoption of improved cyber security practices by business and individuals across Australia's digital economy.

Initiatives such as the ISP Code will encourage ISPs to help their customers improve their online security. The ISP Code will work to support the AISI, which is operated by the ACMA. The AISI provides information to participating Australian ISPs about compromises on their networks with a view to ISPs helping their customers to address the problem. In a similar way, some Australian banks are now offering their customers two-factor authentication to provide enhanced security for higher value online transactions. The Government welcomes these initiatives and is working with industry to encourage demand for and use of more secure IT products and online services amongst Australian business and individuals. For example, the Government is engaging with the banking industry to discuss the development of enhanced fraud and cyber crime prevention capabilities.

Conclusion

The constantly evolving nature of cyber crime will continue to require innovative responses from Government. The rollout of the National Broadband Network will underpin Australia's digital economy; driving productivity, improving education and health service delivery and connecting cities and regional centres. The Government will continue its efforts to help businesses and individuals take advantage of the full range of benefits offered by the digital economy in a secure and confident manner.

The Government thanks the Committee for its report, which will inform the future direction of the Government's efforts to combat cyber crime.

The detail of the Government's response to the Committee's specific recommendations follows.

Recommendation 1: That the Australian Government nominate an appropriate agency(s) to:

- conduct a stock take of current sources of data and research on cyber crime;
- develop clear national definitions and procedures for the collection of data on cyber crime; and
- negotiate clear agreements between government agencies and industry on the sharing and protection of information for research purposes.

Accepted in principle

Stock take of data and research and development of national definitions and procedures

The Government supports these aspects of the recommendation in principle and is considering options for their implementation.

The Australian Institute of Criminology and the Australian Bureau of Statistics (ABS) both have appropriate expertise and the Government considers they would be well placed to undertake the recommended activities in consultation with other relevant agencies. The ABS has recently commenced work on development of a conceptual framework for cyber crime which will define important concepts and issues and provide a common language for analysis and discussion of statistics.
The development of a conceptual framework will serve as a useful starting point for progressing these aspects of the recommendation.

The Government notes that national definitions and procedures for the collection of data on cyber crime would require the agreement of State and Territory governments. Data on crime is currently collected by Commonwealth, State and Territory agencies on the basis of offence type, without a distinction being made on the basis of the mode employed to commit an offence. National definitions that distinguished between, for example, a fraud committed online and a fraud committed by some other method, would entail significant changes to data collection. Accordingly, depending on the definitions adopted, implementation could have considerable resource implications for Commonwealth, State and Territory governments.

Agreements between agencies and industry on information sharing for research

The Government notes existing mechanisms for sharing information between the public and private sectors. For example, CERT Australia maintains agreements with a range of private sector organisations on the sharing of information on cyber security and related issues.

The AFP has developed information sharing agreements with the banking and finance sector, such as through the Joint Banking and Financial Sector Investigation Teams (JBFSITs). In February 2009, the AFP signed an agreement with the Australian Banking Association to allow staff from Australia's major banks to be seconded to the AFP to assist in cyber crime investigations. In addition to industry, the AFP engages in academic outreach activities on the collection of information and data on cyber crime issues.

The Government is also working with industry to develop strategies to enhance fraud prevention. This includes consideration of agreements to facilitate the sharing of information within industry, and between industry and law enforcement, while ensuring that information is appropriately protected to prevent misuse. This work will take into consideration the information sharing frameworks implemented in other countries such as the United Kingdom (UK), where businesses, government departments and law enforcement agencies share detailed data on fraud in real time.

The Government will continue to utilise existing mechanisms and explore new avenues for information sharing between the public and private sectors. The Government will consider the need for specific agreements to cover information sharing for research purposes in the context of work conducted on other aspects of this recommendation.

Recommendation 2: That the Australian Government nominate an appropriate agency(s) to collect and analyse data, and to publish an annual or bi-annual report on cyber crime in Australia.

Accepted in principle

The Government supports this recommendation in principle. Consideration of possible methodology and parameters for regular reporting on cyber crime will be guided by work undertaken to obtain a better picture of current sources of data and research and the outcomes of consultation with State and Territory governments on the development of national definitions and procedures for data collection.

Recommendation 3: That the Australian Government establish an Office of Online Security headed by a Cyber Security Coordinator with expertise in cyber crime and e-security located in the Department of Prime Minster and Cabinet, with responsibility for whole of Government coordination. The Office is to take a national perspective and work with State and Territory governments, as well as federal regulators, departments, industry and consumers.

That the Australian Government establish a National Cyber Crime Advisory Committee with representation from both the public and private sector to provide expert advice to Government.

Accepted in part

Cyber policy coordination

The Prime Minister established the function of CPC within PMC in September 2010. The CPC will provide a single point of policy coordination for issues across the cyber spectrum from consumer protection to cyber warfare.

Advisory Committee

The Government recognises the importance of working cooperatively to combat cyber crime and works closely with other jurisdictions and with industry on cyber crime and cyber security issues through a number of existing mechanisms.

The Government recently established the NCWG, which is comprised of representatives from police services and justice agencies in each Australian jurisdiction. The NCWG will play a key role in ensuring a nationally coordinated response to cyber crime.

From a law enforcement perspective, the Australia New Zealand Policing Advisory Agency (ANZPAA) e-Crime Committee (AeCC) provides a national strategic forum that builds on informal inter-jurisdictional cooperation among e-crime investigators. The AFP also participates in the Five Eyes Strategic Alliance Group Cyber Crime Consultative Working Group which is an internationally represented body that has industry and non-government organisation membership.

The Government is also consulting key stakeholders within the banking industry on the establishment of a high level steering group to discuss the development of enhanced fraud and cyber crime prevention capabilities. These capabilities would enhance the ability of both industry and the Government to respond to a range of crime threats, including technology-enabled crime.

On cyber security issues more broadly, the Government has a number of mechanisms for working cooperatively with the private sector. CERT Australia works with the private sector and industry to share information on cyber threats and vulnerabilities. As part of this role, CERT Australia has established three sector-specific information exchanges with the banking and finance, control systems and telecommunications sectors to enable government and business to share sensitive cyber-security technical information and experiences in a highly trusted environment.

The Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN) enables the owners and operators of critical infrastructure to share information and promote best practice approaches across industry sectors to the management of a range of security and resilience related risks, including cyber security. The TISN's Information Technology Security Expert Advisory Group comprises subject matter experts from within and outside the TISN and provides expert advice to the TISN on IT security issues.

The Government considers that establishing a further advisory committee in line with the Committee's recommendation would duplicate existing efforts. However, the Government will continue working to ensure that existing mechanisms share information and work in partnership where appropriate to support the provision of coordinated expert advice to Government.

Recommendation 4: That the Australian Government, in consultation with the State and Territory governments and key IT, banking and other industry and consumer stakeholders, develop a national online cyber crime reporting facility geared toward consumers and small and medium sized businesses.

This model should include the following features:

- a single portal for standardised online receipt of cyber crime reports across a wide range of cyber crime types (e.g. malware, spam, phishing, scams, identity theft and fraud);
- a 24/7 reporting and helpline;
- no financial minimum to be applied to cyber crime reports;
- systematic data collection that allows data to be aggregated;
- referral to appropriate authorities and cooperation on the disruption of cyber crime and targeted prosecutions;
- free access to scanning software to detect malware;
- public information about cyber crime types and preventative measures to increase online personal security;
- e-security alerts tailored to the needs of ordinary consumers and small and medium sized businesses; and
- analysis of cyber crime methodologies and trends or cooperation with another body to perform that analysis.

Accepted in principle

The NCWG is currently examining arrangements for the reporting of online offences. The NCWG is considering whether these arrangements could be improved through a centralised reporting facility, and if so, the range of functions that the facility could perform.

Recommendation 5: That the Federal, State and Territory police forces establish an E Crime Managers Group to facilitate the sharing of information and cross jurisdiction cooperation.

Accepted

In 2009, ANZPAA established the AeCC, which reports to the ANZPAA Crime Forum. The AeCC is comprised of senior managers of e-Crime from police services in each jurisdiction and a representative from the Australian Crime Commission (ACC). The AeCC is responsible for facilitating effective investigation of e-crime across jurisdictions and sharing of technical information and specialist knowledge.

Recommendation 6: That the Australian Government, in consultation with the State and Territory governments, industry and consumer organisations, develop a national law enforcement training facility for the investigation of cyber crime.

Accepted in principle

The Government recognises the importance of investigation skills keeping pace with technology and supports a nationally coordinated approach to training for law enforcement agencies to effectively investigate cyber crime. The NCWG is considering how cyber crime capabilities could be improved across all jurisdictions, including technical capabilities and training.

Recommendation 7: That the Australian Government consult with major IT security vendors, academia and key industry stakeholders to develop:

- options for establishing a coordinated public-private capacity to provide real time operational information on a wider range of cyber crime types that impact on Australian consumers;
- an 'intelligence hub' that facilitates information sharing within and across industry sectors and provides:
    - longer term analysis on cyber crime methodologies across a range of cyber crime types;
    - education on the preservation of digital evidence; and
    - support to law enforcement agencies for targeted prosecutions in Australia and overseas.

Accepted in principle

The Government recognises the need to improve information sharing on cyber crime threats and is committed to consulting with industry to develop further public-private information sharing avenues.

The Government is currently working with the banking and finance sector to consider opportunities for public-private initiatives to share information in real time on fraud and cyber crime events. This will build on existing collaborative arrangements to share intelligence, such as through the AFP HTCO portfolio.

The AFP currently engages with a wide range of industry representatives in relation to cyber crime, including through the following mechanisms.

- Secondment of team members from the four major banks into the JBFSITs.
- Partnerships with Telstra, Google, the IIA, Microsoft, and other information and communications technology related organisations.

- Work with Telstra to further enhance the AFP's capability in covert internet policing and systems development. Secondments are also used as a basis for facilitating information exchange.

- Engagement with Microsoft and Apple to explore developments in technology and research including provision of technical and technological support. These relationships also facilitate the opportunity to seek expert advice and assistance from security experts on current and emerging threats. These benefits are further enhanced through the placement of an AFP member within the Microsoft campus in Redmond, Washington, in the United States of America.

The Government sees merit in the Committee's recommendation for longer term analysis on cyber crime methodologies and is considering how this could best be achieved. The Government also notes that if a centralised cyber crime reporting facility is implemented (as per recommendation 4), it has the potential to assist both real time operational information sharing and longer term analysis as well as playing a role in supporting targeted investigations.

The issue of digital evidence preservation will be considered by the NCWG.

Recommendation 8: That the Federal, State and Territory Attorneys-General review the existing computer and identity fraud provisions and, if necessary, introduce or amend provisions to ensure consistency across all Australian jurisdictions.

Accepted

The Government recognises the importance of effective and nationally consistent computer and identity crime offences. This is the intent behind the model computer offences agreed to by Commonwealth, State and Territory Attorneys-General in 2001, and the model identity crime offences agreed to in 2008.

The model computer offences were implemented at the Commonwealth level by the *Cybercrime Act 2001* (Cth). The Law and Justice Legislation Amendment (Identity Crime and Other Measures) Bill 2008, which would have implemented the model identity crime offences, lapsed when Parliament was prorogued prior to the 2010 Federal election. The Government has reintroduced the model identity crime offences in the Law and Justice Legislation Amendment (Identity Crime and Other Measures) Bill 2010.

Most States and Territories have computer and identity crime offences in place that are consistent with the model laws. The Government continues to encourage all jurisdictions to adopt the model laws.

The Model Criminal Law Officers Committee is currently reviewing the model computer offences at the request of SCAG. The Commonwealth will notify SCAG of the Committee's recommendation to review the identity crime offences.
Any suggested amendments to the model laws will be considered by Commonwealth, State and Territory Attorneys-General through SCAG.

Recommendation 9: That the Federal Attorney-General, in consultation with State and Territory counterparts, give priority to the review of Australian law and practice and move expeditiously to accede to the Council of Europe Convention on Cybercrime.

Accepted

The Attorney-General and the then Minister for Foreign Affairs announced Australia's intention to accede to the Council of Europe's Convention on Cybercrime on 30 April 2010. Australia is currently in a good position to comply with the majority of obligations under the Convention. The Government is working on the final legislative amendments required for Australia to formally accede.

Recommendation 10: That Australia's cyber crime policy strategically target the underground economy in malicious IT tools and personal financial information; the disruption of botnets and the identification and prosecution of botherders.

Accepted

The Government is developing a more effective legal policy and law enforcement strategy in response to emerging cyber crime threats.

The Government's *Cyber Security Strategy* includes a commitment to maintaining a strong legal framework, investigative and enforcement capabilities and a technically aware legal system to combat the growing challenge of cyber crime

At the national level, the Commonwealth and State and Territory governments, through SCAG, have agreed to develop a coordinated national response to cyber crime. This work will be taken forward by the NCWG.

The Cyber Security Operations Centre (CSOC) and CERT Australia are enhancing the Government's capacity to identify and respond to malicious cyber activity. In particular, CERT Australia works with organisations affected by malicious botnets and other cyber activity to make them aware of available Commonwealth Government assistance. Such assistance could include CERT Australia working with law enforcement and international CERT partners to mitigate malicious botnet activity emanating from overseas.

In the law enforcement context, the AFP has established a dedicated team to investigate the computer offences in Part 10.7 of the *Criminal Code Act 1995* (Cth). This team undertakes tactical level activities targeting cyber criminals within and outside Australia, in cooperation with international law enforcement partners.

Cyber crime is a global challenge and any effective response requires close coordination between law enforcement agencies internationally. To assist Australian law enforcement agencies in this regard the Government is taking steps to accede to the Council of Europe Convention on Cybercrime.

Recommendation 11: That the Commonwealth, State and Territory governments establish a national working group on cyber crime to maintain an ongoing, dedicated mechanism for the review and development of legislative responses to cyber crime.

That the working group take a whole of cyberspace perspective and consider relevant IT industry, consumer protection and privacy issues as well as the criminal law.

Accepted

On 7 May 2010, SCAG met to consider the growing incidence and complexity of cyber crime. Commonwealth, State and Territory Attorneys-General agreed to develop a coordinated national response to cyber crime, including the creation of a national working group to:

- provide advice on whether mechanisms for reporting online offences could be improved, and
- consider other issues relevant to cyber crime, such as spam and malware and powers of search and surveillance.

The NCWG is comprised of representatives from police services and justice agencies in each Australian jurisdiction. At the Commonwealth level, membership also extends to the ACC and CrimTrac.

The NCWG held its first meeting on 28 July 2010, and considered issues referred to it by SCAG including the reporting of online offences and the coordination of law enforcement efforts. It also agreed to undertake a detailed review of capabilities to combat cyber crime, including legislative responses.

The NCWG will consider IT industry, consumer protection and privacy issues where relevant, and will engage with other forums on these related issues as appropriate.

Recommendation 12: That the Australian Communications and Media Authority further increase its access to network data for the purpose of detecting malware compromised computers. This should include active consideration of how to increase access to network data held by global IT security companies and, in consultation with relevant departments, whether legal protections to address commercial, regulatory and privacy concerns are desirable.

Accepted

The Government agrees that access to additional or better quality network data would increase the AISI's effectiveness in the identification and notification of compromised computers in Australia.

General commercial, regulatory and privacy concerns and requirements in relation to data provided to the AISI are addressed though agreements between the ACMA and individual data providers.

The Government will consider ways in which the AISI can increase its access to network data, and will also consider whether additional legal protections to address commercial, regulatory and privacy issues in relation to the AISI should be introduced.

Recommendation 13: That the Australian Communications and Media Authority consider how best the Australian Internet Security Initiative network data might be used to support the threat assessment and emergency response functions of government.

Accepted

The Government notes that AISI data is currently shared with CERT Australia and the AFP, who have the ability to draw upon this data in co-ordinating responses to cyber security incidents and in providing information to CSOC to support its threat assessment functions.

Recommendation 14: That the Australian Communications and Media Authority take the lead role and work with the Internet Industry Association to immediately elaborate a detailed e-security code of practice to be registered under the *Telecommunications Act 1997* (Cth).

That the code of practice include:

- an obligation that the Internet Service Provider provides basic security advice when an account is set up to assist the end user to protect themselves from hacking and malware infections;
- a mandatory obligation to inform end users when their IP address has been identified as linked to an infected machine(s);
- a clear policy on graduated access restrictions and, if necessary, disconnection until the infected machine is remediated;
- the provision of basic advice and referral for technical assistance for remediation; and
- a requirement that acceptable use policies include contractual obligations that require a subscriber to:
  - install anti-virus software and firewalls before the Internet connection is activated;
  - endeavour to keep e-security software protections up to date; and
  - take reasonable steps to remediate their computer(s) when notified of suspected malware compromise.

Accepted in principle

The Government recognises that ISPs are well placed to help their clients with their cyber security needs. ISPs are a conduit to the internet for home users and small businesses and thus can play an important role in improving the online security of consumers.

The Government has worked with the IIA to develop the ISP Code. The ISP Code, which will be implemented in December 2010, provides a consistent approach for ISPs to help inform, educate and protect their customers in relation to cyber security issues. The ISP Code will be reviewed after 12 months of operation.

The ISP Code builds on the AISI, a voluntary initiative which provides participating ISPs with information about compromised computers on their networks. There are currently approximately 80 ISPs that participate in this initiative, representing over 90 percent of the home user market.

The Government will closely monitor the ISP Code and will review its effectiveness. This will include consideration of whether a code registered under the *Telecommunications Act 1997* (Cth) is more appropriate.

In the mean time, as noted in response to recommendation 12, the Government will consider whether additional legal protections to address commercial, regulatory and privacy issues in relation to the AISI should be introduced.

Recommendation 15: That the Australian Government, in consultation with the Internet industry, review the scope and adequacy of s.313 of the Telecommunications Act 1997 (Cth) to promote Internet Service Provider action to combat the problem of malware infected machines operating across the Internet.

Accepted in principle

The Government agrees that there is a need to promote action by ISPs to deal with malware infected computers.

The Government considers that the ISP Code provides a suitable framework for ISPs to take action to combat the problem of malware infected machines. As noted in the response to recommendation 14, the ISP Code will be reviewed for effectiveness after 12 months of operation. This will include consideration of whether other regulatory options are required.

Recommendation 16: That a more integrated model for the detection and removal of malware, built on the Australian Internet Security Initiative, be implemented. The new scheme should involve the Australian Communications and Media Authority, Internet Service Providers, IT security specialists, and end users in a more tightly coordinated scheme to detect and clean malware infected computers.

Accepted in principle

The Government notes the success of the AISI in detecting malware infected computers and agrees that more effort is required to notify consumers and to clean malware infections once they are discovered.

The Government notes the existence of a market in Australia for the provision of anti-virus software and services to clean infected computers.

The role for Government is to help consumers and ISPs be aware of the options to clean infected computers when detected. The Government considers that ISPs that notify customers that their computer is infected are well placed to do this, and have an interest in telling their customers what they can do to clean up their machine.

The ISP Code, which will be implemented in December 2010, will provide a consistent approach across the industry for ISPs to notify and help their customers with malware infected computers.

The ACMA and CERT Australia will further consult with interested parties including ISPs, cyber security specialists and software vendors to examine options to better address the remediation of malware infections.

Recommendation 17: That the Australian Communications and Media Authority be funded to develop a system that can obtain data on compromised web pages from various sources (including developing an internal capability). This data be collated and provided as daily aggregated reports to Internet Service Providers identifying infected web pages residing on their networks.

That in addition to Internet Service Providers, domain owners and hosting companies also be included in the new scheme.

Accepted in part

The Government supports the development of a system to obtain data on compromised web pages which can be aggregated and sent to ISPs and other entities, including domain owners and hosting companies, identifying infected web pages residing on their networks.

CERT Australia is the Government's primary source of cyber security information for the Australian community and the point of contact for Australia's international cyber security counterparts. It provides all Australians with access to information on cyber threats and vulnerabilities so that they can better protect themselves. CERT Australia provides a trusted environment for information exchanges between the Commonwealth Government and business on cyber security related issues and has a coordination role during a serious cyber security incident.

The Government, through CERT Australia, will develop a system to obtain data on compromised web pages which can be aggregated and sent to ISPs and other entities identifying infected web pages residing on their networks. In doing so, CERT Australia will collaborate closely with the ACMA to ensure that this system utilises existing information sources and data developed by the AISI, relevant to compromised websites. The size and scale of this initiative will be informed by an ongoing analysis of the cost and benefit of this system to ISPs and other entities.

Recommendation 18: That the system for reporting and detecting compromised web pages proposed in recommendation 17 be supported by a registered industry code that outlines industry procedures for dealing with infected websites.

That the Australian Communications and Media Authority be empowered to enforce the provisions of the registered code, including, for example, where there is a need to direct a service provider to remove malicious content.

That Internet Service Providers and hosting companies who act on reports of infected websites be indemnified against claims for losses.

Accepted in principle

As outlined in the response to recommendation 17, the development of a system for detecting and reporting of malicious websites will be undertaken by CERT Australia. The development of an industry code to support this system is supported in principle, pending an assessment of the system itself and the ability of industry and government to work together to remediate infected websites detected by the system.
The assessment will inform consideration of whether there is a need for an industry code and, if so, the form that it should take (including whether a registered or non-registered code would be more appropriate).

These considerations will take place in the context of a consolidated regulatory approach for ISPs on cyber security issues. The Government has worked with the IIA to develop a self-regulatory code of practice for ISPs to assist their customers with compromised computers. Any further regulation for ISPs and other internet entities (including web hosting companies) should be part of a holistic approach to address cyber security issues for Australian individuals and businesses.

Recommendation 19: That the Australian Communications and Media Authority and the Internet Industry Association review the Spam Code of Practice to assess the effectiveness of current industry standards for the reporting of spam.

That serious consideration be given to obliging Internet Service Providers to include the Australian Communications and Media Authority's SpamMatters program as part of their email service to subscribers.

Accepted in principle

The Government supports this recommendation in principle and sees merit in the ACMA consulting with industry on the timeframe, process and costs for this review.

The Spam Code of Practice as currently structured does not contain provisions about either customers or ISPs reporting spam to the ACMA. The ACMA considers that these could be usefully considered in a review of the Code.

The mechanisms through which the customers of ISPs and email service providers (ESPs) could make spam reports to the ACMA could be considered in conjunction

with the review of the Code, as well as the costs and benefits of introducing additional spam reporting facilities. Given the different webmail systems operated by ISPs and ESPs these costs are likely to vary considerably between providers. It also needs to be acknowledged that some ISPs currently do not offer webmail services to their customers. The review could also examine the implications of new technologies for reporting spam, with email increasingly being accessed on mobile devices.

Recommendation 20: That the Australian domain name registration industry be subject to a code of conduct that is consistent with the Anti-Phishing Working Group Best Practices Recommendations for Registrars.

The code of conduct should:

- enumerate the type of information that should be collected during the domain name registration process by the registrar, that would help to preserve evidence and assist law enforcement authorities;
- identify processes that should be put in place to identify fraudulent activity before the domain name registration takes effect; and
- provide clear procedures for responding to requests for rapid take down of fraudulent sites and sites that host malware.

Accepted in principle

The Government agrees in principle to explore measures to reflect the principles in the Anti-Phishing Working Group Best Practices Recommendations for Registrars in the management and operation of the Australian domain name space.

It is noted that the Australian domain name space includes:

- '.au', which relates to Australia
- '.cc', which relates to the Cocos (Keeling) Islands
- '.cx', which relates to Christmas Islands
- '.hm', which relates to the Heard and McDonald Islands, and
- '.nf', which relates to Norfolk Island.

Given the system of industry self-regulation in Australia, the Government will consult with law enforcement, privacy groups, industry and the Australian domain name administrators (including, but not limited to, the .au Domain Administration Limited (auDA)) on the implementation of this recommendation.

It is noted that the Anti-Phishing Working Group Best Practices Recommendations for Registrars shares similarities with the due diligence and Registrar Accreditation Agreement amendments proposed to the Internet Corporation for Assigned Names and Numbers by international law enforcement agencies, including the AFP.

Recommendation 21: That the Minister for Broadband, Communications and the Digital Economy make a reference to the House of Representatives Standing Committee on Communications to inquire into the regulation, standards and practices of the domain name registration industry in Australia.

Accepted in principle

The Government supports transparency in the process of managing domain names in Australia. The Government will initiate an external review of the .au country code Top Level Domain administration in conjunction with the .au Domain Administrator (auDA). The Board of auDA will commission an independent expert to conduct a review of auDA's governance arrangements, recognising the unique circumstances of internet management arrangements, and working with the Department of Broadband, Communications and the Digital Economy. The review report will subsequently be made available to the Committee.

Recommendation 22: That the Australian Government ensure that:

- remedies available under the new Australian Consumer Law can be effectively asserted against perpetrators outside Australia; and
- the Foreign Judgments Act 1991 (Cth) be amended to allow for the reciprocal registration and enforcement of non-money judgments made under the Australian Consumer Law.

Accepted in principle

From the date of its commencement on 1 January 2011, the new Australian Consumer Law (ACL) will be able to be effectively asserted against overseas perpetrators.

The ACL will be a schedule to the existing *Trade Practices Act 1974* (TPA), to be renamed the *Competition and Consumer Act 2010* (CCA) on 1 January 2011, and be a law of the Commonwealth and of each State and Territory.

The ACL contains core consumer protection provisions, enhanced enforcement powers, new penalties and improved consumer redress options. The remedies and penalties available under the ACL include those which currently exist in the TPA, such as civil remedies (for instance, compensatory orders and injunctive relief) and criminal sanctions (including fines of up to $1.1 million), as well as new civil pecuniary penalties, public warning notices, disqualification orders and non-party redress. For instance, a regulator can issue a public warning notice where there is reasonable grounds to suspect a supplier may have breached the ACL.

The ACL will apply to conduct engaged in outside of Australia that is in trade or commerce, by virtue of subsection 5(1) and section 6 of the CCA, by bodies corporate who are incorporated in, or carrying on a business in, Australia, or by Australian citizens or persons ordinarily resident within Australia. For example, the ACL would apply to overseas conduct directed towards or intended to be accessed by Australian consumers, including conduct engaged in over the internet in trade or commerce.

Part 2.7 of the *Criminal Code Act 1995* (Cth) will also apply to offences in the CCA. This has the effect of applying those offences where conduct constituting the offence occurs outside Australia if a result of that conduct occurs in Australia.

Under subsections 5(3) and 5(4) of the CCA, the Commonwealth Minister can grant or withhold consent to legal proceedings concerning conduct engaged in overseas that would breach the Act, subject to foreign law and national interest considerations.

Effective enforcement of domestic consumer protection laws overseas can be difficult even when overseas perpetrators are located. This is because leave from the court must first be sought to serve the documents. Australia's recent accession to the Hague *Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* will simplify and harmonise the procedures for transmitting and serving Australian court documents in the many member states to this Convention. However, difficulties may continue to exist in relation to countries not covered by this Convention and who do not have any other transmission and service arrangements with Australia. In addition, the utility of court orders may be undermined by the difficulty in enforcing the orders against an overseas respondent in their jurisdiction. Due to some of these practical difficulties, the Australian Competition and Consumer Commission (ACCC) relies on other methods to disrupt unlawful conduct of overseas perpetrators, including:

- taking action against intermediaries based in Australia, such as cheque clearing houses
- disrupting methods of delivery, including working with Australian ISPs to remove problematic websites, and
- naming identified scams, businesses or individuals for consumer awareness and education.

Equally important is the use of international cooperative efforts for the effective enforcement of consumer protection laws against overseas conduct targeting Australian consumers. To this end, the Committee noted existing arrangements between the ACCC and international consumer protection enforcement authorities through the International Consumer Protection and Enforcement Network (ICPEN). The Committee also noted the bilateral agreement the ACCC has with the United States Federal Trade Commission on Mutual Enforcement Assistance in Consumer Protection Matters. The ACCC also has a number of memoranda of understanding with other agencies to facilitate international cooperation, including with agencies in Canada, Korea, New Zealand, Papua New Guinea and the UK.

The Government agrees in principle that it would be desirable to examine avenues that could lead to greater enforceability in Australian courts of orders resulting from proceedings in which foreign courts have applied the ACL. Expanding the scheme created by the *Foreign Judgments Act 1991* (Cth) is one such avenue, but one which may be of limited effect in the context of providing comprehensive protection for Australian consumers under the ACL.

These limitations arise because the Foreign Judgments Act relies on the concept of 'substantial reciprocity of treatment', which can only be ascertained through often

complex bilateral processes; it cannot be achieved by unilaterally amending the scheme. Also, the scheme applies only to a limited range of foreign judgments. Criminal sanctions or criminal and civil pecuniary penalties would not be covered by the scheme.

Australia has long recognised the importance of effective international arrangements for the recognition and enforcement of civil and commercial judgments and will continue to pursue such arrangements in a range of bilateral and multilateral forums, including through organisations such as the Hague Conference on Private International Law.

Recommendation 23: That the Treasurer amend the Australian Consumer Law to include specific protections against the unauthorised installation of software programs:

- the reform should target the unauthorised installation of programs that monitor, collect, and disclose information about end users' Internet purchasing and Internet browsing activity;
- the authority to install a software program must be based on informed consent; and
- to obtain informed consent the licence/agreement must require clear accessible and unambiguous language.

Accepted in principle

The Government believes it is important there are adequate protections available to Internet users, including protecting end users' personal information and browsing activity. As noted by the Committee, some existing provisions of the TPA (and the ACL from 1 January 2011) apply to the conduct targeted by this recommendation, and may mean that specific protections of the type recommended may not be necessary.

The unfair contract terms (UCT) provisions of the ACL ensure that consumer agreements are based on informed consent and that such agreements are clear, legible and transparent.

The UCT law provides that unfair terms in standard form consumer contracts are void and unenforceable. These provisions commenced on 1 July 2010 as a law of the Commonwealth and of New South Wales and Victoria, and will apply in all other States and Territories from 1 January 2011. A standard form consumer contract is one that is for the supply of goods or services acquired wholly or predominantly for the purpose of personal, domestic or household use or consumption. This could include a software installation agreement.

A term is unfair if it would cause a significant imbalance in the parties' rights and obligations under the contract, is not reasonably necessary to protect the legitimate interests of the party who would be advantaged by the term, and would cause detriment (financial or non-financial) to a party if it was relied on. A relevant consideration as to whether a term is unfair is its transparency; that is, whether the term has been expressed in plain language, presented clearly, is legible and readily available.

In addition, the Committee noted the prohibitions against false, misleading or deceptive conduct in the ACL also help to ensure that consent is based on correct, clear and unambiguous information.

The unauthorised installation of a software program which proceeds to collect and disclose information about the end user's internet purchasing and browsing activity is likely to contravene the National Privacy Principles (NPPs) of the *Privacy Act 1988*.

In particular, NPP 1.2 provides that an organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way. In addition, an organisation that unlawfully collects personal information by means of unauthorised monitoring software in breach of NPP 1, is also unlikely to be mindful of their other obligations in relation to handling personal information. This could give rise to issues under other NPPs, such as NPP 2 (use and disclosure), NPP 3 (data quality), NPP 4 (data security), NPP 5 (openness), NPP 6 (access and correction), NPP 8 (anonymity) or NPP 9 (transborder data flows).

Pursuant to sections 5B and 6C of the Privacy Act, the NPPs only apply to organisations which are Australian based or carrying on a business in Australia. The definition of organisations excludes small businesses, registered political parties, Australian Government agencies and State or Territory authorities. The organisation must also either be Australian based or carrying on a business in Australia.

As a general rule, the ACL as a generic law is intended to encompass all products (including software programs) and all industries (including the IT industry), with industry-specific regulation only added when necessary. Implementation of the ACL is a key regulatory reform priority under COAG's *National Partnership Agreement to Deliver a Seamless National Economy* (November 2008). The ACL is subject to the *Intergovernmental Agreement for the Australian Consumer Law* (IGA), which was signed by COAG in July 2009. The IGA commits the Australian and the State and Territory governments to repeal, amend or modify any legislation that is inconsistent with, or alters the effect of, the ACL. This includes both general consumer protection legislation and more industry-specific provisions.

The IGA provides a process for amending the ACL, including formal voting arrangements for proposing legislative change. Under the IGA, all proposals for legislative change require the support of the Commonwealth and four other jurisdictions, at least three of which must be States.

The Government will discuss this recommendation further with State and Territory Ministers responsible for the ACL.

Recommendation 24: That the Australian Competition and Consumer Commission, in consultation with manufacturers and distributors of personal computers, mobile phones and related IT devices such as modems and routers, develop information standards to:

- address the e-security vulnerabilities of these products and the provision of e-security information to consumers at the point of sale; and
- require that the information is presented in a manner that is clear and accessible to a non-IT literate person.

Accepted in principle

The Government considers that manufacturers and distributors of personal computers, mobile phones and related IT devices, such as modems and routers, should be encouraged to provide generic cyber security information to consumers at the point of sale. This generic information could be drawn from publically available sources including the Australian Government's *Stay Smart Online* and *SCAMwatch* websites and the *Protecting Yourself Online – What Everyone Needs to Know* booklet.

The Government will, in the first instance, encourage manufacturers and distributors of personal computers, mobile phones and related IT devices, such as modems and routers, to develop voluntary information standards before considering a mandatory approach under the ACL. In this regard, the Government is particularly conscious of the need to ensure information is current in a fast-changing IT environment and the risk that formal requirements may become quickly outmoded.

Under the ACL, the Commonwealth Minister may make mandatory information standards in relation to the supply of goods and services. This includes the power to make a standard that require suppliers of specific kinds of goods to provide certain information about those goods to consumers, and the power to require such information to be presented in a particular manner or form. There are currently no information standards that apply to the IT industry.

New information standards made under the ACL must be agreed to by the required number of States and Territories under the IGA. Generally, a new industry-specific mandatory information standard is only desirable in circumstances where industry has failed to voluntarily provide certain information necessary to inform consumers about the nature or quality of a particular product.

Outside of the ACL, there have been several activities to rationalise the number of mandatory product labels and reduce regulatory overhead for suppliers of devices. The introduction of electronic labelling within the technical regulatory framework was one such means of providing additional flexibility for suppliers to label their products.

Recommendation 25: That the Treasurer direct the Productivity Commission to conduct an in depth investigation and analysis of the economic and social costs of the lack of security in the IT hardware and software products market, and its impact on the efficient functioning of the Australian economy.

That, as part of its inquiry, the Productivity Commission address the merits of an industry specific regulation under the Australian Consumer Law, including a scheme for the compulsory independent testing and evaluation of IT products and a product labelling scheme.

Accepted in principle

The Government agrees that an in depth analysis of the economic and social cost of cyber crime and other cyber security risks on the Australian economy would be a useful input into further policy development. However, the Government does not

consider the Productivity Commission (PC) to be the appropriate body to conduct a review of the kind recommended. The PC has a broad role and expertise in matters of microeconomic reform and productivity. A specialist body with greater knowledge in the areas of IT and e-commerce, such as a consultant or expert panel, may be better placed to conduct a review. To this end, the Government will consider commissioning an expert consultant to undertake a review.

In its *Review of Australia's Consumer Policy Framework* (2008), the PC recommended that the COAG Business Regulation and Competition Working Group, in consultation with the Ministerial Council on Consumer Affairs, review existing industry-specific regulation in Australia on consumer policy. The PC noted that overlaps between industry-specific regulation and generic consumer laws are not always supported by a demonstrated need, and in some cases the regulation is overly prescriptive. The PC was also of the view that inconsistencies between industry-specific regulations in different jurisdictions imposed unnecessary compliance costs on businesses, and that those regulations which overlap with more generic consumer laws should be removed.

Under the IGA for the ACL, the Australian, State and Territory governments have agreed to repeal, amend or modify any legislation that is inconsistent with, or alters the effect of, the ACL, including industry-specific laws.

Industry-specific consumer legislation that attempts to regulate IT hardware and software based on technological developments is a challenging proposition. Technology will continue to evolve independently of any legislation that can only attempt to regulate a subset of its uses. Efforts to introduce consumer regulation that address specific technological challenges may allow new technologies to enter the marketplace without providing adequate protection of consumers who use those technologies.

Recommendation 26: That the Treasurer consult with State and Territory counterparts with a view to amending the Australian Consumer Law to provide a cause of action for compensation against a manufacturer who releases an IT product onto the Australian market with known vulnerabilities that causes losses that could not have reasonably been avoided.

Accepted in principle

Existing provisions of the TPA are relevant to the conduct targeted by this recommendation. The implied conditions and warranties provisions of the TPA require suppliers to ensure that, amongst other things, their goods sold are free from any known fault or defect that has not been disclosed to the consumer. Similar provisions exist in State and Territory fair trading and sale of goods legislation.

A new system of statutory consumer guarantees, based on the existing implied conditions and warranties provisions of the TPA, will operate as part of the ACL and apply in every State and Territory from 1 January 2011.

The new statutory consumer guarantees regime improves the legal framework for consumer rights that apply to the acquisition of goods and services. The new regime

makes it easier for all Australian consumers and suppliers to understand their rights and obligations in consumer transactions, supported by effective redress options. The ACL includes a statutory guarantee that goods, including IT products like pre-packaged software, are of acceptable quality, free from any defects and are fit for purpose.

Provisions in the ACL that prohibit false, misleading or deceptive representations being made about the nature, characteristics, standard or quality of a product, may also apply, depending on the nature of any representation made by a software supplier to a consumer.

As the ACL will be applied in every State and Territory by way of application laws, consumers will be able to enforce their rights under the ACL through relevant state courts and tribunals, in addition to the Federal Court of Australia and the Federal Magistrates Court.

Remedies available to affected consumers include damages for loss suffered, and, where a statutory guarantee has been breached, the supplier may be required to refund, replace or repair the product in question. The ACL also allows enforcement agencies to obtain redress for non-parties.

In addition, suppliers may also face a civil pecuniary penalty of up to $1.1 million if they contravene provisions of the ACL (for instance, if the supplier has made a false or misleading representation).

Recommendation 27: That the manufacturers of IT products adopt a best practice approach that ensures products are designed to prompt and guide end users to adopt more secure settings.

That the Australian Government monitor industry practice in this regard, and promote international standards that put a higher priority on security through product design.

Accepted

The Government agrees that it is desirable for manufacturers of IT products to take a best practice approach that encourages and makes it easier for end users to adopt more secure settings.

The ACCC will engage with the significant manufacturers of IT products to encourage best practice in the design of products and provision of information to consumers regarding securing settings. This will include discussion of international best practice, such as the adoption of more secure settings at the point of supply. Engagement will also focus on encouraging the supply of information by manufacturers at point of sale and in packaging to provide guidance to consumers on how to adopt more secure settings.

This will be complemented by information on these issues being made available on the ACCC website, including general information for consumers on how they can safely purchase IT hardware.

Recommendation 28: That the Office of the Privacy Commissioner use the full extent of its powers to ensure that overseas organisations that handle the personal information of Australian citizens and residents are aware of, and adhere to, their obligations under the *Privacy Act 1988* (Cth).

Accepted

The *Privacy Act 1988* (Cth) applies to acts done or practices engaged in outside Australia by an organisation if the act or practice relates to the personal information of an Australian citizen or permanent resident, and the organisation is either:

- an Australian organisation, or
- an organisation that carries on a business in Australia and collects or holds the information in Australia.

The powers available to the Australian Information Commissioner under Part V of the Privacy Act apply to complaints against organisations that fall within these parameters. The Government has accepted the Australian Law Reform Commission's (ALRC) recommendation to amend the Privacy Act to clarify that it also applies to acts done or practices engaged in outside Australia by Australian Government agencies.

On 24 June 2010, the Government released an exposure draft of the new Australian Privacy Principles, which were referred to the Senate Finance and Public Administration Committee for public consultation and report. The Australian Privacy Principles form the first part of the Government's first stage report to the ALRC Report. Proposed Australian Privacy Principle 8 deals with the cross-border disclosure of personal information. To assist public understanding of the Australian Privacy Principles, the Government also released a companion guide. The Committee is due to report by 1 July 2011.

The Government also recognises the importance of active and constructive engagement with the privacy and information protection regulators of other nations and economies. The Office of the Australian Information Commissioner (into which the Office of the Privacy Commissioner has been integrated) is an active member of and participant in forums such as the Asia Pacific Privacy Authorities forum, the annual International Conference of Privacy and Data Protection Authorities, and the Electronic Commerce Steering Group of the Asia Pacific Economic Community (APEC). Australian Government agencies have also been involved with the Organisation for Economic Cooperation and Development Working Party on Information Security and Privacy.

In addition, the APEC Cross-border Privacy Enforcement Arrangement (CPEA) took effect on 16 July 2010. The CPEA sets out a framework for voluntary cooperation and assistance between participating authorities on privacy enforcement-related activities. It enables the Office of the Australian Information Commissioner to obtain assistance from, and give assistance to, foreign privacy enforcement authorities to resolve complaints and investigations with a cross-border element (such as those involving overseas-based organisations).

The Government is committed to ongoing international cooperation to mitigate cyber security risks.

Recommendation 29: That the Office of the Privacy Commissioner expedite the adoption of an approved privacy code of practice for members of the Australian Internet industry, including smaller Internet Service Providers.

Accepted

The Government supports development of an approved privacy code of practice for members of the Australian internet industry, but notes that it is the role of industry, not the Office of the Australian Information Commissioner, to develop such a code.

The Australian Information Commissioner has the power to approve a privacy code when an organisation applies for such approval. However, the Australian Information Commissioner currently does not have the power to prepare a privacy code or approve a code in the absence of a relevant application.

The Government notes that, although the IIA has previously prepared a draft code and made an application for approval, that application has not been pursued. The Office of the Australian Information Commissioner is prepared to expedite the application if the IIA wishes to recommence the application process.

Recommendation 30: That the Office of the Privacy Commissioner encourage government agencies and commercial organisations to undertake regular audits to identify risks to personal information in both new and existing projects and policies.

Accepted

As noted by the Committee, the Government has accepted the ALRC's recommendation that the Office of the Australian Information Commissioner be empowered to direct agencies to provide Privacy Impact Assessments (PIAs) for new projects or for developments that the Australian Information Commissioner considers may have a significant impact on the handling of personal information.

The Office continues to advocate the use of PIAs and provides a Privacy Impact Assessment Guide to assist agencies and organisations in assessing the privacy impact of projects. This was revised in May 2010 to include a module for private sector and not-for-profit organisations.

Recommendation 31: That the Department of Broadband, Communications and the Digital Economy, in consultation with relevant agencies, industry and community organisations, develop a nationally coordinated strategy for the education of consumers:

- that the strategy cover all aspects of cyber crime including malware, identity theft, identity fraud and scams; and
- includes clear benchmarks against which the effectiveness of education initiatives can be clearly evaluated and publicly reported on to Parliament.

Accepted in principle

As noted by the Committee, a range of Government agencies undertake awareness raising activities in this space. The Government recognises the need for a coordinated approach to education and awareness. It has taken steps through initiatives such as the *Protecting Yourself Online – What Everyone Needs to Know* booklet and the Stay Smart Online website to provide consumers with consistent and coordinated messages for a safer and more secure experience online.

The Government will explore how best to achieve better coordination on education and awareness, which will include considering the development of an enhanced national strategy. Such a coordinated approach would need to provide a framework for consumer education and awareness on cyber security, cyber safety, cyber crime and other online risks such as privacy issues.

Recommendation 32: That the Stay Smart Online and SCAMwatch websites be linked to the national cyber crime reporting centre referred to in recommendation 4.

Noted

The Government agrees that a more integrated approach should be taken to the provision of cyber security information to end users. As noted in the response to recommendation 4, the NCWG is currently considering whether existing arrangements for the reporting of online offences could be improved through a single reporting facility. If a single reporting facility is established, the Stay Smart Online and SCAMwatch websites could be linked to the facility.

Recommendation 33: That the Department of Broadband, Communications and the Digital Economy implement a public health style campaign that uses a wide range of media to deliver messages on cyber security issues, technical precautions and appropriate user behaviours.

Accepted in principle

How the Government targets different audiences will be examined as part of the coordinated approach described in the response to recommendation 31. In developing a coordinated approach to education and awareness, the Government will consider the most effective means of bringing about the desired online behavioural change within

the Australian community. This would include detailed consideration of implementing a public health style campaign and other potential options.

Recommendation 34: That the Department of Broadband, Communications and the Digital Economy support the development of IT literacy training that includes cyber security and is available to the community as a whole.

Accepted in principle

The Government recognises the value in providing training that includes cyber security elements to members of the community.

The Government will consider the education needs of various target audiences in education and awareness as part of the coordinated approach described in the response to recommendation 31. The need for IT literacy training would be considered as part of this.