Supplementary Submission No. 34.1

House of Representatives Standing Committee on Communications Inquiry into Cyber Crime: additional Questions on Notice
Department of Broadband, Communications and the Digital Economy

Domain Name System

1. **What enforceable obligations exist to ensure domain name registrars and resellers verify the identity of IP address applicants?**

The Internet Corporation for Assigned Names and Numbers (ICANN) is the international not for profit, multi-stakeholder body which is responsible for the accreditation of Registrars for the generic Top Level Domains (gTLDs), such as '.com', '.net' and '.info'.

At present there is no requirement on ICANN accredited Registrars to verify the identity of registrants, although in many cases the use of an alias would be a breach of the terms and conditions of registration.

ICANN maintains legally binding contracts with Registrars, which outline a number of obligations for Registrars. For example, the Registrar Accreditation Agreement (RAA) provides that Registrars must submit to ICANN data such as the name and addresses of registrants and the IP addresses of the primary and secondary name servers used by the registered name.

ICANN has no authority to accredit the Registrars that operate in the country code Top Level Domains (ccTLDs), such as '.au', '.nz' and '.uk'. Each country has different systems in regulating their ccTLDs.

The .au Domain Administration (auDA) is responsible for the accreditation of Registrars that take reservations for domain names in '.au'. auDA is the private sector, not for profit corporation responsible for the administration of the .au name space.

Under subclause 9.1.2 of auDA's non-negotiable Registrar agreement, Registrars must use reasonable endeavours to verify the information provided in Domain Name Applications. Equally, under auDA's published policies registrants must warrant that the information that they provide is true, accurate and complete. auDA has advised that a 'warranty' provided by the Registrant is considered sufficient. In the industry itself there are a range of mechanisms used, some for instance ask for ACN or ABN numbers (although it is not known whether these Registrants check this information against the ASIC database for instance).

Nevertheless, the issue of identity verification in the .au name space is recognised as an important issue by the Department of Broadband, Communications and the Digital Economy and auDA. auDA has undertaken to consider how identity verification procedures could be improved.

Neither auDA nor ICANN have direct contractual relationships with resellers. However, in both the gTLDs and .au resellers operate under an agreement with their Registrar, which must include minimum terms and conditions.

2. **What enforceable obligations exist to ensure that an Australian domain name registrar will remove a domain name that is, for example, associated with phishing?**

General domestic Australian laws, such as the Crimes Act 1900, the Criminal Code 1995, and the Trade Practices Act 1974, may apply to the conduct of Registrars, depending on the specific jurisdictional circumstances. Provisions relating to theft, unauthorised access and misleading and deceptive conduct may apply to Registrars that are complicit in a breach of these laws.

auDA's Registrar Agreement provides that the registrar must comply with all applicable laws.

Please see auDA's published policies at (www.auda.org.au/policy/current-policies/) for further information.

3. **Is Australia represented in the Internet Corporation for Assigned Names and Numbers (ICANN) structure and, especially, in any forum concerned with e – security?**

ICANN is a multi-stakeholder forum, and is private sector led. Governments participate in the ICANN process through the Governmental Advisory Committee (GAC). The Australian Government was a founding member, and has participated in the GAC since 1999.

While the Australian Government is not eligible to formally join other security focused committees in ICANN (such as the Security and Stability Advisory Committee), it does provide input into these processes, including through the GAC.

A number of Australians are involved in various fora within the ICANN, however they do not represent Australia in this capacity.

4. **ISPs want immunity from liability for losses incurred arising from good faith actions taken to protect the integrity of the network. However, the industry appears to be unclear about existing legal protections:**

    a. **Can the Department confirm that section 313 of the *Telecommunications Act 1997* applies to ISPs and the online environment?**

Section 313 of the *Telecommunications Act 1997* (Telco Act) places several obligations on carriers and carriage service providers. To the extent that an Internet Service Provider (ISP) is a 'carriage service provider' for the purposes of the Telco Act, it will be obliged to comply with the obligations imposed under subsections 313(1) and (3). These obligations arise in connection with the ISP's operation of telecommunications networks and facilities, and their supply of carriage services. Specifically, subsection 313(1) relates to preventing telecommunication networks and facilities from being used to commit offences against Commonwealth/ State/Territory laws. The obligation under subsection 313(3) relates to giving reasonably necessary help to Commonwealth/State/Territories officers/authorities for the purposes of enforcing the criminal law and laws imposing pecuniary penalties, protecting the public revenue, or safeguarding national security.

If the ISP (in its capacity as a carriage service provider) does any act (or omits to do any act) in good faith as part of fulfilling one of the duties it has under subsections 313(1) or (3), it will be immune from civil action for damages in relation to that action (or omission) - refer subsection 313(5)(a). A similar immunity is extended to the officers, employees and agents of a carriage service provider (refer subsection 313(6)).

The immunity also applies to circumstances where an ISP (in its capacity as a carriage service provider) undertakes action in compliance with a direction by the Australian Communication and Media Authority (ACMA) (refer subsection 313(5)(b). This is discussed in part c below.

Where an ISP's actions in the 'online environment' are correctly characterised as being in connection with the supply of a carriage service, or the operation of a telecommunications network by the carrier, the obligations under section 313 will therefore have application.

b. If not, has the Government considered providing a similar protection to good faith actions taken in the online environment?

Please refer to above answer.

c. Would registration of the E-Security Code of Practice under the *Telecommunications Act 1997* assist in indemnifying ISP's acting on reports of compromised machines from ACMA?

The registration of the Code by the ACMA will not, in itself, give the ISPs immunity from civil action for damages in relation to any action the ISPs may undertake in relation to acting in accordance with the Code. However, if the ACMA, in performance of its duties under section 312, issues a written direction to the ISP to comply with the Code for the proposes of preventing telecommunications networks and facilities from being used in, or in relation to, the commission of offences against the laws of the Commonwealth and of the States and Territories, an immunity may be afforded. This is the case, provided that the ACMA gives the direction in good faith.

Similarly, where the action undertaken by the ISP in compliance with Code is correctly described to be action that the ISP is undertaking in good faith in fulfilment of its obligation under subsections 313(1) or (3), then the immunity will also be afforded. [For example, it could be argued that the act of responding to reports on compromised computers (e.g. computers with trojans/malware) could be considered to be reasonable action undertaken by the ISP to prevent its telecommunication networks and facilities from being used to commit cybercrimes under Commonwealth laws.] If that is the case, then the obligation under 313(1) or (3) applies to the ISP, as would the immunity under 313(5)(a) for the reasonable acts undertaken. As you will appreciate, the immunity is linked to the broad obligations under 313 or an ACMA direction issued in the performance of its duties under section 312.

It is important to note that the proposed code at this stage will be voluntary. The effect of registering an industry code, such as the proposed E-Security Code, under Part 6 of the Telco Act means that the ACMA can make directions to any participant in the particular section of the telecommunications industry to which the Code relates to comply with it, and there are fines for not complying, see section 121.

Infection of Legitimate Websites

5. **ACMA has said that criminals are targeting and infecting legitimate websites with malware as basis for launching other attacks, and this is now the number one issue that must be addressed to adequately respond to cyber crime:**

    a. **What consideration did the E Security Review give to this issue and how does the Government propose to respond to this new trend?**

The E-Security Review 2008 (Review) considered a broad range of cyber risks including, specifically, the issue of criminals targeting and infecting websites for malicious purposes. The Review identified that further exploration of legal issues associated with this problem is required. This work will be taken forward by the Cyber Security Policy and Coordination (CSPC) Committee agencies. The CSPC Committee, which is chaired by the Attorney General's Department, is the interdepartmental committee that coordinates the development of cyber security policy for the Australian Government.

More broadly, the Government's Cyber Security Strategy recognises that the risk to the Australian economy from computer intrusion and the spread of malicious code by organised crime has been assessed as high.

The Government is undertaking a number of measures to address this issue, including:

- creating the new national computer emergency response team, CERT Australia. As part of its functions, CERT Australia will provide a trusted environment for information exchanges between government and business on cyber security issues. It will also work with other national CERTs around the world, the IT industry and Australian Internet service providers to help network operators to identify and respond to cyber security incidents,
- providing additional resources for security and law enforcement agencies to enhance operational capabilities for combating cyber crime and other cyber security threats, and
- ensuring that linkages are in place between cyber security and law enforcement efforts to combat specific related crime types, including organised crime, through the sharing of information and intelligence.

    b. **What new resources and powers will be provided to ACMA to address the problem of infected websites?**

As mentioned above, the Cyber Security Policy and Coordination Committee agencies will further explore legal issues associated with the problem of infected websites. This work will guide any allocation of new resources and powers as required.

Personal Malicious Online Activity

6. **There is a host of malicious online activity that adversely affects a person's sense of personal security, privacy, and reputation and blurs the lines between the criminal law, privacy and defamation. Not all malicious activity will reach the threshold of a criminal offence or warrant expensive defamation proceedings:**

    a. **Given the pervasiveness of new communications technologies, is it time to provide individuals with a statutory right to make a complaint about violations of privacy and malicious attacks on reputation?**

There are several avenues available to consumers that apply to violations of privacy and malicious material and conduct including:

Criminal Code

The *Criminal Code Act 1995* states that it is an offence to use a carriage service (a telecommunications or Internet service) to communicate in a way that is regarded as menacing, harassing or offensive. All State and Territory police have the authority and power to charge a person with this Commonwealth offence.

Australian Human Rights Commission

Anti-discrimination legislation, such as the *Racial Discrimination Act 1992, Sex Discrimination Act 1984, Age Discrimination Act 2004, and Disability Discrimination Act 1992*, may apply to online content. Parallel legislation exists in all States and Territories.

The Australian Human Rights Commission is an independent statutory organisation that can investigate complaints of discrimination, harassment and bullying based on a person's:

- sex, including pregnancy, marital status, family responsibilities and sexual harassment;
- disability, including temporary and permanent disabilities; physical, intellectual, sensory, psychiatric disabilities, diseases or illnesses; medical conditions; work related injuries; past, present and future disabilities; and association with a person with a disability;
- race, including colour, descent, national or ethnic origin, immigrant status and racial hatred;
- age, covering young people and older people; or
- sexual preference, criminal record, trade union activity, political opinion, religion or social origin (in employment only).

State and Territory defamation laws

Further, the States and Territories have their own defamation laws which may apply to online content. Information about the defamation laws is available for each State and Territory.

Privacy Act 1988

The Office of the Privacy Commissioner (OPC) has complaint handling responsibilities under the *Privacy Act 1988*. If individuals believe that their privacy has been interfered with by an Australian or Australian Capital Territory government agency, or a private sector organisation covered by the *Privacy Act*, they may make a complaint to the OPC. The *Privacy Act* does not apply to State and Northern Territory government agencies or bodies, including local councils,

however State and Territory privacy laws may apply. The *Privacy Act* also does not apply to media organisations acting in the course of journalism, or individuals acting in their own capacity.

The Australian Law Reform Commission (ALRC) undertook a comprehensive two year review to consider whether, in light of the rapid changes in information technology, privacy is adequately protected in Australia. In its final report *For Your Information: Australian Privacy Law and Practice* (Report 108) released on 11 August 2008, the ALRC recommended that Australia should introduce a statutory cause of action for a serious invasion of privacy. The ALRC anticipated that the action would be available for interferences of privacy in both the online and off-line environment by individuals, organisations or Government agencies.

When the report was released, the Government noted that it would be considering the recommendations of the report in two stages with the statutory cause of action to be considered in the second stage. The Government has recently released its first stage response on the report and will be releasing exposure draft legislation to implement those reforms in early 2010. Consideration of the second stage reforms will occur once the first stage implementation is well progressed.

Australian Communications and Media Authority's role

It should be noted that regulation of online content does not expressly cover unauthorised malicious images or statements, intended to ridicule, defame or otherwise harm a victim. Under Schedule 7 to the *Broadcasting Services Act 1992* (BSA), the ACMA has the power to direct an Australian hosting service provider to take-down content that is prohibited content (or in certain cases take action to ensure that the content is not prohibited content). Prohibited content is defined in clause 20 of Schedule 7 to the BSA, with reference to the National Classification Scheme categories set out in the *Classification (Publications, Films and Computer Games) Act 1995* (Classification Act), and includes:

- content that is classified Refused Classification (RC) or X18+
- content that is classified R18+ and not subject to a restricted access system
- content that is classified MA15+, not subject to a restricted access system, and provided on payment of a fee.

The National Classification Scheme is a portfolio responsibility of the Minister for Home Affairs. The ACMA asks the Classification Board to classify content that has been the subject of a complaint when the ACMA is uncertain of the appropriate classification. In the case of content that is hosted in Australia, the ACMA must ask the Classification Board to classify content that is likely to be prohibited.

The Classification Board's guidelines state classifications are to be determined with regard to the impact of the material in question. Factors such as whether material is unauthorised, defamatory, intended to cause harm to a person or ridicules a person may have some bearing on its impact and classification, but are not likely to be primary determinants of its classification.

The ACMA does not have power under the BSA to direct removal of prohibited content that is hosted outside Australia. Instead such content is added to a list of URLs that is provided to filter software vendors. This arrangement is set out in a code of practice for ISPs that is registered under the BSA. The Government has also recently announced the introduction of mandatory ISP level filtering for overseas hosted RC content.

Telecommunications Industry Ombudsman

The Telecommunications Industry Ombudsman (TIO) is a free and independent alternative dispute resolution scheme for small business and residential consumers in Australia who have been unable to resolve their concerns directly with their telephone or internet service provider. Alternative dispute resolution is a means of settling a dispute outside a courtroom. It is a more accessible and informal way of resolving a complaint and the TIO's role is to help consumers and telecommunications companies resolve complaints together. The TIO has jurisdiction to investigate complaints on a range of telecommunications matters including privacy.

b. Should we give the Privacy Commissioners and ACMA the power to order removal of online content that is malicious (e.g. unauthorised publication of an image, an intentionally harmful posting that defames a young person)?

The ALRC considered in Chapter 11 of its privacy report *For Your Information: Australian Privacy Law and Practice* (Report 108) whether the scope of the *Privacy Act 1988* should be extended to allow the Office of the Privacy Commissioner to issue take-down notices about privacy invasive content online. The ALRC did not make a recommendation on this issue as it considered that there were other methods (including the recommended statutory cause of action) which more appropriately would deal with this issue, particularly in situations where an individual is acting in a personal capacity when he or she interferes with another individual's privacy. The Government is therefore not currently considering this issue in its privacy reforms.

With regard to the *Broadcasting Services Act 1992* (BSA), such a proposal would depart from the objectives of the online content scheme under the BSA, which are based on the regulation of content over other media and not designed to address malicious or defamatory content. The primary objective of the online content scheme is that providers of content services should be required to respect community standards and to establish measures that protect children from exposure to content that is inappropriate or harmful for minors.

Please also refer to response to 6.a above.

Reliable Research Data

7. ACMA has pointed out that, while there is plethora of reports on the extent of the problem of malware, there is limited independent information available:

a. What role will the Department play in establishing an independent research effort on the problem of malware and the existence botnets in the Australian network to provide consistent and reliable evidence for policy makers?

The Department's role in establishing an independent research effort is limited to the Department's portfolio responsibility. The Department has from time to time undertaken research on cyber security related issues. For example, the Department commissioned KPMG to develop cyber security threat and vulnerability assessments for home users and small businesses in 2006 and 2008.

Community IT Literacy

8. **Some witnesses have advocated a nationally consistent approach to IT literacy, in the school room, at work and at home. The European Computer Drivers Licence appears to be widely adopted in the EU and international version is available in Australia:**

    a. **Has the Department considered the merit of the European/International Computer Drivers Licence and working with the Australian Computer Society to promote IT literacy using this model?**

We understand the International Computer Driving Licence (ICDL) operates internationally and is also based in Australia. We also understand that the IDCL modules do not include specific units on cyber security. At this stage the Department has not considered working with Australian Computer Society to promote IT literacy using this model.

However the Department recognises the importance of IT and digital media literacy to the development of Australia's digital economy. This has been acknowledged by the Australian Government in the Australia's Digital Economy: Future Directions paper published in July 2009. The digital economy is essential to Australia's productivity, global competitive standing and improved social wellbeing. Digital media literacy is identified in Australia as one of the measures of a successful digital economy.

In relation to cyber security, the Department runs a range of cyber security awareness initiatives to help home users and small businesses take simple steps to more secure and confident online. One of the key initiatives is the cyber security schools education package, also know as the Budd:e Package. This package consists of two self-learning and interactive online modules for students in years three and nine.

The development of the Budd:e Package was informed and supported by the ICT in Schools Task Force and is consistent with the Ministerial Council on Education, Employment, Training, and Youth Affairs (MCEETYA) Statements of Learning for ICT. A Reference Group of teachers and curriculum experts was established to inform the development of the Package. The Package was also tested and piloted in 22 selected public, private and independent schools around Australia before it was launched in June 2009.

The Department is also involved in the provision of a comprehensive package of measures as part of its Cyber-Safety Plan. This includes extensive education and outreach activities provided by ACMA. The Government has recently announced further measures to continue and expand cyber-safety education and awareness activities which support the key role parents and teachers have in the online safety of children. These will assist parents and teachers to help children understand cyber-safety risks, including cyber-bullying. This funding will also reduce waiting times for schools to participate in ACMA's cyber-safety outreach program and increase the Cyber-Safety Online Helpline operating hours to ensure it is available when children are most at risk.

Community Awareness

9. **Several witness have suggested a public health styled media campaign (e.g. the skin cancer 'slip, slop, slap' campaign) to communicate key e-security message and achieve real cultural change among end users:**

    a. **What do you consider the most effective way of communicating the e-security message to the wider public?**

Public health style media campaigns are certainly effective vehicles for communicating messages to the community. Many public health messages are clear-cut and delivered in a powerful and often shocking manner. This is not a workable option in the case of cyber security messages. Given the significance of the digital economy to the Australian community, messages about cyber security need to be delivered in such a way that they do not scare people away from engaging in the online world.

However, public health media campaigns entail other elements that can be usefully applied to cyber security awareness raising. For example, most public health media campaigns are sustained over a long period of time. To this end, the Department is partnering with stakeholders to reach the community throughout the entire year. In addition to the Cyber Security Awareness Week, the Department is delivering a cyber security festive season initiative to raise awareness of secure online practices whilst shopping or banking online (November – December 2009) and a back-to-school cyber security awareness campaign (January – February 2010). The Department also partnered with the Australian Telecommunications Users Group in August and September 2009 to deliver awareness messages to community groups across Western Australia, New South Wales and Tasmania.

    b. **Does the Government intend to adopt a broad based electronic media campaign to promote personal internet security? If not, why not?**

The Department is partnered with stakeholders from industry, government, community groups and consumer groups. Such partnerships have helped the Department to garner media exposure to promote its awareness messages. For example, during the 2009 National E-security Awareness Week, circulation and audience figures for items appearing on television, radio and in print and online media were estimated to be around 3.4 million.

The next Cyber Security Review is scheduled to take place in 2010 at which time the Government will assess its cyber security policies and programs. Our current awareness program will be assessed during the course of this review. All possible options will be considered to improve the current program.

    c. **What would the key messages of a broad based campaign be?**

For cyber security messages to be effective, they need to be simple, easy to adopt and consistent. Five key messages consistently delivered through current initiatives are as follows:

- Get a better, stronger password and change it at least twice a year
- Get security software, and update and patch it regularly
- Stop and think before you click on links or attachments from unknown sources
- Information is valuable. Be careful about what you give away about yourself and others online
- Log onto www.staysmartonline.gov.au for further information and sign up for the email alert service.