SUBMISSION NO. 42

Australian Government

Department of the Prime Minister and Cabinet

HOW TO MAKE A SUBMISSION

To participate in this consultation, you need only answer those questions below of interest. Please keep additional commentary short and succinct.

Should you wish, submitters are also invited to provide demographic information to assist in analysing peoples' response. This information will be anonymised and aggregated and further information on how the Department of the Prime Minister and the Cabinet manages your information can be found at www.dpmc.gov.au/privacy.cfm.

Please use the submission template attached to this paper.

Submissions can be sent by email in.doc, .docx, .rtf or .pdf format to cyberwhitepaper@pmc.gov.au. Please keep submissions below 10 Megabytes in size. Submissions can also be lodged at our website, posted or faxed.

WEBSITE

http://www.cyberwhitepaper.dpmc.gov.au

POSTAL ADDRESS

PO Box 6500
CANBERRA ACT 2600
Australia

FAX

6271 5414

Unless you clearly request confidentiality, **submissions may be public documents** and may be accessed by any member of the public, may be published on a website and quoted in further review papers. If you do not want your submission to be published, or you would like to request anonymity, you must clearly request this in your submission.

Do you agree to your submission being used publicly by the Cyber White Paper Team in the final White Paper, additional reports, conference presentations and associated publications?

Yes ☒ No □

Submissions must be received by close of business **14 November 2011**. Submissions received after this date may not be able to be considered.

Australian Government

Department of the Prime Minister and Cabinet

Additional demographic information

Gender: Male

Age: 65+

State: NSW

Submission provided on behalf of: Individual

Frequency of online usage: 21+ hrs per week

Occupation: N/A

Digital citizenship in a networked society

Issue*: A growing portion of our lives and civic experience is conducted in the online environment. This environment has a unique set of characteristics, including anonymity, and allows people to interact socially unhindered by geographic distance.*

- **Question**: How can we promote a concept of digital citizenship, reach agreement on acceptable online behaviour and encourage people to assume greater responsibility for that behaviour?

Support Australian media producers to introduce infotainment into their productions that highlights digital citizenship. Advertisements have little lasting impact these days, however stories always have and do. The modern day story is now delivered by television.

Issue*: The online environment can create a sense of dislocation from our actions; the ability to act anonymously online can embolden bullies and sometimes abusive, offensive or illegal behaviour can go unchecked.*

- **Question**: How can governments, the private sector, the NFP sector and the broader Australian community work together to promote responsible and accountable digital citizenship and reduce harassing and malicious online behaviour?

Support Australian media producers to introduce infotainment into their productions that highlights the impact of poor online behaviour. Online actions are really no different to phone calls or anonymous letters, except more immediate, low cost and difficult to track.

Issue*: Children and young adults are prolific users of social networking sites and as a result can be exposed to a range of online risks, including abusive behaviour.*

- **Question**: How can we help carers and parents to appropriately supervise young people and minimise these online risks?

1. Provide parents and carers with suggested settings for the more popular sites. These suggested settings would need to be available online and quickly updated. They should be set out in different scenarios - eg settings to protect children's safety yet still allow maximum learning; settings for adults that protects their privacy and sensitive personal details. Where a decision might be either way on a setting, then explain the pros and cons. For less popular sites provide general guidelines of suggested settings.

2. Educate the parents as explained throughout this submission.

- **Question**: How can we promote social responsibility and encourage young people to protect themselves and each other by speaking out against cyberbullying?

1. Support and encourage Australian media producers to introduce infotainment into their productions that highlights the importance of reporting cyber bullying, how unsociable it is, the impact on victims, how a victim should handle it and the consequences for perpetrators when caught.

2. Continue school programs and advertisements against bullying.

Issue*: Social networking sites are almost entirely facilitated by the private sector. Although many of the larger sites have some capacity to monitor and limit abusive behaviour, some others do not.*

- **Question**: How can the owners of social networking sites be more engaged in meeting community expectations that their platforms will not be used for abusive or illegal activities?

Have a qualified and independent panel review each site and provide positive suggestions to the site owner (attempt to establish a formal relationship with them). If serious enough then publicise those site owners who ignore or dismiss these suggestions. Extending the existing Scamwatch system would be one way.

Issue*: Social networking sites and increased social connectivity provide increased opportunities for people to collaborate, share ideas and produce socially valuable outcomes.*

- **Question:** What new and innovative opportunities do social networking tools provide to improve the social well-being of Australians?

1. The ABC is a leader in using Facebook for gathering opinions and increasing the sharing of ideas. Consult them.

2. Online groups and forums baffled me at first, however once I understood how they worked, the benefits to me and how I could help others, then they are great. This is an area that needs more promotion and education.

3. The biggest impediment is lack of knowledge about systems and how they can be of benefit.

- **Question**: How can NFPs ensure the security of online fundraising activities conducted through social networking sites?

The government could assess and publish systems that it deems secure and suitable for fundraising. Another possible extension of Scamwatch.

I encourage the use of proven systems like Paypal where personal financial details are only ever exposed to one entity whose reputation totally relies on security.

Issue*: Governments are progressively implementing online services in response to community expectations. However, many individuals do not trust their private data will be appropriately managed.*

- **Question:** How can governments improve citizens' and businesses' trust that their private data will be secured and only used for agreed purposes?

1. Explain why the private data is being kept and give real life examples of how it is of benefit, particularly to individuals. People are largely driven by self interest.

2. Give some examples of what is involved to access the data. For example how will a Doctor or nurse access peoples health records, hopefully not just by password, but by both password and security card; or fingerprint or iris recognition.

3. There will always be breaches and abuses and these should be promptly, openly and honestly reported, dealt with, rectified, and steps put in place to prevent future events.

4. Cut the vocal chords of some of the sensationalism driven shock jocks and current affair shows. Some of these media outlets are no better than 'Chicken Littles' and the unknowing listeners are easily led to believe their fears. 'MediaWatch' needs to be more widely promoted.

5. A suitably qualified independent authority tasked with listing, reviewing, assisting and accrediting all Australian based data stores. Another possible extension for the Scamwatch authority.

Protecting and promoting Australia's digital economy

Issue*: The digital economy presents both wide-ranging opportunities for increased productivity and innovation across the Australian economy and the risk of the loss of sensitive commercial data.*

- **Question**: How can small business awareness of commercial online opportunities be balanced with awareness of potential online risks and mitigation strategies?

1. Enlarge and promote Scamwatch so it is more proactive in explaining what antivirus programs there are, their pros and cons; what a firewall is and how to implement it; how to check if your security is adequate; the importance of backup.

2. Targeted education of business owners, particularly small business.

- **Question**: How can governments, industry, NFPs and consumer groups boost consumers' confidence to engage in e-commerce?

1. More war stories about success and failure stories. Why they succeeded and why others failed.

2. See if its possible to have infotainment type programs like those on Landline, RBT (Random Breath Testing)

Issue*: Industry and governments need to strike the right balance between improving awareness of and protecting against cyber threats, while also encouraging consumers to take advantage of the benefits of the digital economy.*

- **Question**: How can governments and the private sector continue to build and maintain confidence in the digital economy while also raising awareness among consumers and small businesses of the nature of cyber threats?

1. I feel that many in the workforce are ignorant of computers, the internet, online trading, backing up, systems etc and this is seriously impacting Australia's productivity as well as cyber safety. This is often not the fault of the people, particularly small businessman, technology and systems have evolved rapidly and many have not had the time to keep pace or can envisage the benefits. Again, this is an education problem and needs to be both targeted and cost and time efficient. Refer to later submission about surveys of small businesses.

2. Many could make better use of free cloud systems such as Google documents, however many are not aware of them and their benefits of collaborative work, inbuilt security and backup.

- **Question**: How can we improve and encourage the reporting of data breaches in Australia?

Have one overall independent authority - eg Scamwatch. The government should take the initiative rather than waiting for some industry based system to evolve with little intent other than self interest.

- **Question**: How can e-businesses more effectively work together to develop a self regulatory feedback system that provides a way of sharing their experiences with other online traders?

1. Investigate what current forums exist. www.Whirlpool.net.au is a great example of an active forum that has gone beyond just internet topics. Another is www.productreview.com.au.

2. If suitable, I suggest Scamwatch start a moderated forum. Membership restricted to online traders so that scam artists don't paste false info and also the forum stays focused on traders needs

3. Educate online businesses about the advantages of forums. Stress to businesses that its not about sharing their business model, but about sharing protection ideas and war stories for the common good.

Issue*: Police resources are finite and cyber crime investigations are inherently time and resource intensive. Consequently, the growth in cyber crime activity poses significant challenges to Australia's state and territory and federal police services.*

- **Question**: What does the Australian public expect from policing and consumer protection agencies in relation to preventing and investigating cyber crimes?

They expect full protection, however they don't want the pain of learning!! Its similar to how many expect complete protection of their business and houses without taking the basics of locking their doors!

The question should be 'How do we make peoples expectations real?' Scamwatch supplies very good factual information - it needs wider and ongoing coverage and support. Infotainment is another avenue to get it across that what the perpetrators say about who they are and where they are has no connection to reality.

***Issue**: One of the primary impediments to e-commerce is consumers' fear their financial or personal details may be at risk when conducting business online. Anonymity will remain a key part of the Internet, but trust and confidence in the digital economy may be undermined if people's financial and personal details remain at risk of being stolen by criminals.*

- **Question**: What options are there for increasing consumers' trust in conducting business online?

EBay has a good model where feedback on transactions is encouraged by all. Traders are given a % rating that is a good indicator of a traders honesty. Many traders will go out of their way to ensure they retain a high rating. EBay also promotes the Paypal guarantee.

- **Question**: How can consumers be encouraged to take more responsibility to protect their information?

Infotainment. Encourage Australian produced shows to work in storylines showing poor cyber practices and/or actions and the consequences and costs of rectifying the result.

- **Question**: What are the options for broadening industry's efforts to provide customers with a greater level of trust and confidence in the security and privacy of their online transactions?

Encourage more consistent, and promotion of FAQ pages for buyers to check. Develop suggested FAQ formats. Question and answer format is an easy way of clearly presenting information.

- **Question**: What information would help consumers and small businesses better protect themselves and enhance their trust and confidence online?

Simple things like publish ideas on how to make an easy to recreate password. Complex passwords advocated by some in the IT business maybe very secure, however they are useless as people can't remember or easily recreate them.

- **Question**: What do consumers and small businesses expect from their Internet Service Providers (ISPs), software and hardware providers and the government to assist them to maintain or enhance their confidence online?

The ISP's, software and hardware providers are all commercial entities. No matter how well they do there is always the suspicion that that will be promoting a particular action or product. Further, they often introduce their own sales terms as if they were the only method. Government sites such as Scamwatch, or non profit like Choice would be seen as more reliable and free of sales bias.

- **Question**: How can governments and industry work together to make Australia a difficult place for cyber criminals to target?

Relevant EDUCATION of users. Users need to become 'defensive drivers' on the cyber highway.

***Issue**: Damaging criminal activities are often aided by the use of botnets, built as a result of many individuals unwittingly operating virus-infected computers. The Australian Federal Police estimate that the overall risk of cyber crime to the Australian economy is more than a billion dollars a year. This is likely to grow substantially as Australia's digital economy expands.*

- **Question:** What are the options for limiting the collective economic and societal costs of widespread individual security lapses?

1. Again, education is prime.

2. A reliable source of accurate and relevant information about items like an easy to recreate password, free anti-virus software.

- **Question:** What role do individuals, businesses and, more specifically, ISPs and large online companies, have in limiting the collective harm compromised computers have on the Australian economy and to the broader well-being of the Australian community?

They all have a role, and should be encouraged, however their primary interest is themselves.

***Issue**: The effects of cyber crime and scams often extend beyond the immediate financial impacts. Many instances of online crime go unreported, so the full extent of the problem is not known.*

- **Question**: How can Commonwealth and state and territory governments encourage victims to report incidences of cyber crime and scams and better assist them with support and advice?

Scamwatch should enlarge their victim stories section to show ALL reports, the outcome, what the user should have done both before and after the scam.

- **Question**: How can Commonwealth and state and territory governments obtain the information and data required to form a more precise assessment of the extent of the economic and social harm caused by cyber crime?

Centralised collection point - eg Scamwatch

***Issue:** Small businesses often lack access to the security controls employed by government or other larger enterprises, yet consumers expect small businesses to secure their data and transaction appropriately.*

- **Question:** How can government, ISPs, financial institutions and small businesses collaboratively create an environment where small businesses are empowered to operate in a safe and secure manner online?

Centralised collection point - eg Scamwatch. The Internet, scammers and cyber criminals know no boundaries. Its a Commonwealth obligation

Security and resilience in the online environment

***Issue**: Much of the public discussion on cyber threats and risks to date has focused on national security issues. This important dimension has inadvertently hidden the reality that at its most basic level, security and safety online is reliant on the awareness of individuals. As a result, many businesses and consumers are not as mindful of cyber threats as they could be.*

- **Question**: How can the Commonwealth, states and territories and industry effectively communicate the interdependent nature of individual and national cyber security? How can the importance of individual behaviour be highlighted in creating a secure, trusted and resilient online environment for all Australians?

Basic computer and internet usage and risks EDUCATION. Free for the basics.

- **Question**: How can citizens better protect themselves from cyber threats?

Participate in the EDUCATION above. ‘Most’ know the importance of wearing a seatbelt; of not drinking and driving; of having a new car insured; of protecting their valuables. ‘Most’ also learn after they have been the victim of an attack or have been scammed, however its often not positive learning, ie they become averse to future trading.

- **Question**: Are individuals adequately aware of cyber threats and the steps they should take to protect themselves? If not, why not?

Aware of threats - yes; Steps to take - definitely not. In dealings with relatives, friends, some small businesses, computer club members and BFS students I often find:

- expired or no anti-virus protection

- unpatched software and no idea why its important to do so. Users often ignore or dismiss the software update prompts

- failure to backup valuable personal and business items

- clicking without thinking

Reasons for their behaviour are:

- lack of basic computer knowledge;

- financial restrictions;

- attitude of ‘it’s all too hard, it won’t happen to me’;

- unawareness of alternatives to expensive software and equally expensive upgrades;

- confusing sales methods by anti-virus sellers.

- unawareness of Scamwatch and its offerings

I would like to see the results of some spot surveys done of some pockets of local small businesses to ascertain their vulnerability, level of knowledge, backup plan, online trading experience and practices etc. Has any of this been done?

Such surveys should also be used to target the training of small businesses. What are their needs? What were the major shortcomings found? Suggestions for fixing the suggestions. What resources are available to them?

International partnerships and Internet governance

***Issue**: The attractions of the internet in terms of openness, access to information (of all qualities) and informal governance are also creating tensions with traditional government responses to community interests.*

- **Question**: What model of Internet governance is in the best interests of all Australians?

1. Education of users on safe surfing, reliability of information, what to be aware of.

2. Support and encouragement of free or lost cost software that is readily available. A very reliable site for this is Gizmo's site set up by Australian Ian Richards at www.techsupportalert.com I'm quite sure he would welcome some financial support to keep this site running. In 2010 it was nominated by PC Authority magazine as one of the Top 100 websites.

Some examples of free quality software that I swear by: Microsoft Security Essentials; CCleaner, MalWareBytes and Web Of Trust (WOT). Gizmo recommends these 9 must have free programs at http://download.techsupportalert.com/9-great-freeware-programs.pdf

- **Question**: How can we get the right balance between Australia's social, economic and security needs when developing an Australian vision for the online environment?

I always remember one expert being asked whether the roadside breath testing limit should be 0.05 or 0.08. I though his answer of 'It doesn't matter' the dumbest answer until he added '....the whole point is to change peoples attitude to drink driving'. Changed attitude is also the answer to safe Internet usage. Trying to regulate its usage is impossible unless you adopt the totally unacceptable approach of China. That leaves education (proactive) or penalties for perpetrators (reactive)

***Issue**: Increasingly, policy makers have turned to discussing what agreements governing behaviour in the online environment might look like, the principles they should be based on, the boundaries they would place on behaviour and how they can be promoted. This will be a gradual and long-term process, and different stakeholders are likely to want different outcomes from any agreement.*

- **Question**: What sort of approach should be taken to developing agreements on behaviour in the online environment?

I feel that trying to regulate or put boundaries on peoples usage is impossible. That is like trying to regulate that people in Sydney are only able to drive within a 150 km radius of Sydney. Politically unpopular and impossible to regulate unless all roads have checkpoints. The Internet is no different.

Investing in Australia's digital future

***Issue**: The demand for skilled cyber professionals in both the public and private sector will continue to grow at a rapid rate and it is likely that those companies – many of which will be based overseas – offering the best financial incentives will attract the best of Australia's ICT graduates. However, a purely market-led distribution of skilled cyber workers may not meet the broader digital needs of Australia as a nation.*

- **Question**: What strategies should be pursued by governments, industry and academia to ensure adequate levels of domestic expertise are available to maximise the opportunities of the digital economy and address risks to Australia's digital infrastructure?

The NBN is an essential to promote the notion of living in Australia with its lifestyle and tele-commuting with far away places in real time.

- **Question**: What new forms of government-industry cooperation and dialogue are required to ensure the Australian cyber skills base is developed to meet Australia's broader national interests?

Industry and government could be more proactive in providing scholarships and traineeships that lock students into working for them for say 12 months at the completion of their studies. Our son had one from BHP that enabled him to do his PhD. Whilst his thesis was work that BHP could benefit by there, and he did work for BHP during it, there was nothing to lock him to Australia. The university &/or BHP were also very bureaucratic and slow in processing the scholarship.

***Issue**: Australians' level of digital literacy is growing, yet many elderly and vulnerable Australians are unaware of the opportunities and risks inherent in digital technologies.*

- **Question**: How can we ensure all sectors of the Australian community have the necessary skills and security awareness to optimise the benefits of the digital economy?

1. Extend the BFS concept to the wider community with paid part time tutors. Some ideas on how this could be run are:

a. There are many experienced computer users in the retired community who could provide this tuition. There are also many school kids who, with suitable training on how to tutor, that could do this. All would welcome the extra money. We had one unemployed school leaver at the Muswellbrook Computer Club who volunteered to do tutoring. His computer knowledge was very good, all we had to do was sharpen up his shyness and communication skills and the seniors loved him. This also gave him valuable work like experience which we were happy to write references for and enabled him to pick up paid employment.

b. Put these kiosks in shopping centres. Others in venues that provide after hours and weekend access. I suggest a pilot scheme in a couple of communities to trial this. (Suggestion: Use some of the computers at those Internet Cafe kiosks that are in larger shopping centres and are charging 21 minutes for $2.)

c. Wherever possible, users should be encouraged to learn on their own computers as many have laptops. This

- reduces the need for training hardware,

- enables them to continue learning after the training session without the confusion of different hardware, desktop and programs,

- allows problems such as expired antivirus to be assessed and rectified,

- allows tuning of settings that may be hampering the student - eg overactive mouse, too fast a double click speed, help for people with handicaps.

d. Proposed training kiosks should offer free wifi and ethernet access. To prevent abuse, access could be both time and capacity limited as is done at McDonalds. As all networking devices have a unique MAC address then this could also be used to limit abuse and overuse by personal computers.

e. Offer at home training for handicapped and elderly. The Brisbane Seniors OnLine offer this type of training for all members and have done so for sometime http://www.bsol.asn.au/pages/

f. Basic training could be free, donation or a very low nominal cost.

2. Investigate, support and advertise online self paced training systems such as developed by ALA for the BFS system. These are in need of review an updating - eg the Windows 7 interface for WordPad is now the %&*@ ribbon.

I am currently investigating the free Alison system at http://alison.com/course/ and another two that look promising are http://inpics.net/ and http://www.gcflearnfree.org/ I intend starting to build a list of these resources for the BFS. If deployed on a larger scale then such a list would need review by others and then could be more widely publicised.

3. Many of the formal training entities - eg TAFE etc seem to concentrate on courses that provide industry oriented courses, cost money, have a rigid curriculum, require travel and are classroom run. My experience with the BFS, Muswellbrook Computer Club and training relatives and friends is that most new starters require almost individual instruction to get them over initial fears and the new terms. Just like learning to ride a bike, or the clutch in a car, requires that initial one to one assistance to gain the skill.

***Issue**: Being viewed as a world leading digital economy in the way that Singapore is in our region, is critical to attracting overseas investment, both in our ICT sector and more broadly because of the enabling role of digital technologies.*

- **Question**: Besides rolling out the NBN, what role does the government have in promoting opportunities for individuals and businesses to compete in the global information communications technology marketplace and to increase the attractiveness of Australia as a destination for digital investment?

Our youngest son got an excellent Australian education to PhD level, then had to leave Australia as nobody was doing the sort of scheduling programming he was interested in. Currently he is living in Edmonton and tele-computing with his employer in Vancouver. The NBN will open up this avenue even more for people to stay in Australia. The government could do more to show exactly what is possible. Again, infotainment might be the best avenue to reach the mass of people as to what will be possible.