SUBMISSION NO. 30

Australian Government
Department of Veterans' Affairs
OFFICE OF THE SECRETARY

Mr James Catchpole
Committee Secretary
Joint Select Committee on Cyber-Safety
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Mr Catchpole

Thank you for your letter of 8 December 2011 regarding the Select Standing Committee's inquiry into cyber-safety for senior Australians. I appreciate having the opportunity to provide a written submission to the inquiry.

From your letter, I understand that many senior Australians may not be using the internet due to concerns about their safety when online. In addition, those senior Australians who do use the internet are susceptible to increased risks and threats when using online technology.

The Department of Veterans' Affairs (DVA) has a number of clients who would be considered 'senior Australians'. DVA utilises a range of options for communicating with its clients, including letters, face-to-face contact, the telephone and online communication. Online communication may occur via the use of email for receiving and sending correspondence or through social networking sites, such as Facebook, or tools like Twitter. In most cases, the method of communication used will be that preferred by the individual client. Therefore, if a client is not comfortable communicating using online technology, traditional forms of correspondence and information sharing continue to be available.

The Department is aware of the types of risks facing senior Australians online. One of the most common scams targeted at our clients is where people pose as DVA or Government officers to elicit personal information which can then be used to commit identity fraud or make financial gain. For example, clients have been asked to provide personal information, including bank account details, in order to access a Government grant or rebate. Other clients have been advised of an overpayment of benefits and asked to repay the debt to DVA, in addition to a processing fee, using money transfer. In most cases, these scams were perpetrated by way of a phone call or a letter, rather than email. This tends to highlight a perception in the broader community that veterans and war widows prefer traditional forms of communication to online communication. However, this is certainly not true of all clients, irrespective of age. Furthermore, clients using the internet may still be exposed to these scams online. For example, where they receive an official-looking email purporting to be from DVA or are directed to a fake website where they are asked to verify personal or financial information.

LOVETT TOWER
13 KELTIE STREET
PHILLIP ACT 2606

GPO BOX 9998
CANBERRA ACT 2601
AUSTRALIA

TELEPHONE (02) 6289 6736
FACSIMILE (02) 6289 6257

The Department seeks to raise awareness of the need for good information and communications technology security, including avoiding scams. On becoming aware of the scams targeted at our clients, the Department sought to raise awareness in the veteran community. Two articles were published in separate issues of *Vetaffairs*, a newspaper published four times a year by DVA and distributed to more than 300,000 members of the veteran and defence force community and available online. The first article provided details of the scams, while the second article focused on identity theft, how it can occur and ways to prevent it. Both articles directed people to contact DVA in the event that they were asked for personal information and provided the link to the Government's 'Scamwatch' website, which provides useful information on protecting privacy.

In addition, the Department has a 'Scam information' page on its website (http://www.dva.gov.au/help/Pages/scams.aspx), which details scams specifically targeting its clients, as well as the general community. It provides the following information on protecting one's identity:

Identity theft prevention measures:

- Keep key documents secure at home and when travelling;
- Only carry essential information;
- Destroy personal documents before disposing of them;
- Put a lock on your letterbox;
- Activate Caller ID on your phone and note any suspicious calls;
- When banking online, check the 'closed padlock' symbol is displayed;
- Never access a banking site through a link in an email;
- If it sounds too good to be true, it usually is;
- Never provide account details in order to receive winnings/prizes;
- Choose strong, obscure passwords using a mix of letters, symbols and digits and change them regularly;
- Avoid giving personal information over the phone or internet;
- If suspicious of a caller, get the caller's name, title, and a number, and offer to call back;
- Use wiping or erasing software before selling or disposing of your computer. Simply deleting files or formatting the hard drive is not enough; and
- Be suspicious of callers requesting personal information in exchange for new government services such as free electricity or pension benefits.

Senior Australians may also be exposed to online bullying and harassment through the dissemination online of incorrect information. The Department is aware of the Australian and New Zealand Military Imposters (ANZMI) website, which publishes material seeking to expose individuals who purport to be veterans. The Department and Minister for Veterans' Affairs have received correspondence from people who are concerned by information that has been posted on the ANZMI website about themselves, family members, friends or others in the veteran community. Without commenting on the veracity of the information published on the website, it is noted that people are unaware of what avenues may be open to them where they consider the internet is being used improperly.

The Department supports any awareness campaigns or education programs to reduce the exploitation of senior Australians online. Programs could be aimed at educating senior Australians in how to safely use a computer and the internet and in increasing their skills in these areas. For example, people should be encouraged to install security software on their computers, but also be

informed of the importance of regularly changing online passwords, using a variety of different passwords and not sharing that information with anyone else. People could be directed to the Scamwatch website, so that they can become familiar with the types of scams they may encounter and information could be made available regarding what to do if they experience harassment online. Furthermore, senior Australians should be educated on how to protect themselves online and when using the internet. Once people understand how and why their personal information can be obtained and used, they will be better equipped to protect it.

I note that the Department of Families, Housing, Community Services and Indigenous Affairs administers the 'Broadband for Seniors' initiative. This is currently being used by a number of ex-service organisations which host internet kiosks where veterans can receive tutoring in how to use a computer and the internet. It is recommended that this initiative be continued and expanded to include tutoring on the risks of online communication and awareness of cyber-safety. The initiative could be further advertised during National Cyber Security Awareness Week, with particular events targeted at senior Australians.

This type of education could be extended to those senior Australians who do not consider themselves at risk from online threats, because they do not use a computer or the internet. Those people who are not familiar with the internet are unlikely to be aware that their personal information is online, even when they themselves may not be, and that it can be used in scams against them. Information including a person's name, address and phone number is likely to be on the internet where it is also listed in a hardcopy phone book. People who work or volunteer with community organisations may also have their details listed on the organisation's website.

The Department of Broadband, Communications and the Digital Economy is best placed to develop educational materials and programs for senior Australians. I understand that it has already produced material about online risks for young Australians. I consider this could be used as the basis for developing material targeted at senior Australians and the risks unique to them as a user group. The 'Stay Smart Online' website has areas dedicated to, for example, children and teenagers and an area dedicated to senior Australians could be developed. By increasing awareness of the types of internet scams and information uses in existence, senior Australians will be better equipped to protect themselves from online risks and threats and, therefore, be more likely to engage in using online technology.

I commend the Committee for conducting this important inquiry and look forward to seeing the results of the inquiry in its report.

Yours sincerely

Ian Campbell
Secretary

19 March 2012