

14 November 2011

To the Department of the Prime Minister and Cabinet

Via e-mail: [cyberwhitepaper@pmc.gov.au](mailto:cyberwhitepaper@pmc.gov.au)

Re: Australia Cyber Discussion Paper

Dear Sirs,

Congratulations for the progress and issuance of the Cyber Discussion Paper, *Connecting with Confidence*. Among other things, this discussion paper begins to outline a vision for Australia's digital future based on Australian values. ISACA applauds the Australian government for making the issue of cybersecurity a strategic imperative for the country. ISACA continues to follow the development of this global issue and we very much appreciate the opportunity to provide comments and recommendations to the Department of the Prime Minister and Cabinet. These comments and recommendations are offered on behalf of ISACA<sup>®</sup> and the IT Governance Institute<sup>®</sup> (ITGI<sup>®</sup>), international, independent thought leaders on information technology (IT) control, security, risk, assurance and governance of enterprise IT.

We believe the Department of the Prime Minister and Cabinet's discussion paper will be useful to start the dialog—from the viewpoints of both the enterprise and the "person on the street." We look forward to the issuance of the Australia White Paper on Cyber Issues next year. Our general comments are provided in the following section of the letter and our responses to the full, detailed questions outlined in the discussion paper are included in Attachment A.

### **General Comments**

We are very supportive of Australia's Cyber Discussion Paper. We have limited our detailed comments to those areas of the discussion paper we believe will have the greatest impact and that represent the areas of greatest interest for our membership. We offer the following general thoughts:

- Consider expanding cybersecurity education to create a technically skilled and cybersavvy workforce.
- Investigate building a rigorous workforce certification system, which would include creating a governance body, based on a federated model, focused on certifications in two or three specialty areas. This governance body would evaluate whether any current certification programs meet the requirements. The board would consist of major private sector organizations, universities, key federal government agencies and independent not-for-profit (NFP) professional bodies such as ISACA.

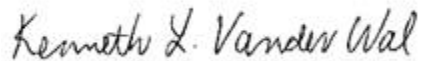
\* \* \* \*

As the worldwide leading independent thought leaders on security, assurance, IT risk, governance and controls, we are eager to assist the Australian government in accomplishing its goals with regard to cybersecurity. ISACA truly appreciates the opportunity to comment on the discussion paper and we thank you for considering our views. We would be happy to discuss them with you in further detail and provide any other assistance that might be required to ensure that your efforts to provide a safe and secure cyberinfrastructure are successful and lasting.

Two Australian ISACA members, who also serve on the ISACA/ITGI Board of Directors/Trustees, and their contact information follow:

- Tony Hayes, CGEIT; Board of Directors—International Vice President, Brisbane resident. Phone number 0412.153.071
- Jo Stewart-Rattray, CISM; Board of Directors—International Vice President, Adelaide resident. Phone number 0418.818.867

Respectfully submitted,



Kenneth L. Vander Wal, CISA, CPA, International President  
ISACA ([www.isaca.org](http://www.isaca.org)), IT Governance Institute ([www.itgi.org](http://www.itgi.org))

### **About ISACA and ITGI**

With 95,000 constituents in 160 countries (over 2,850 in Australia), ISACA members have developed, implemented, managed and assessed security controls in leading critical infrastructure organizations and governments on a global basis. ISACA is a leading global provider of knowledge, certifications, community, advocacy and education on information and systems assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. ISACA continually updates COBIT<sup>®</sup>, which helps IT professionals and enterprise leaders fulfill their governance and management of IT responsibilities, particularly in the areas of security, risk, assurance and control to deliver value to the enterprise. COBIT is used within many governmental departments and regulatory bodies around the world. ISACA also participates in the development of international security standards through its liaison status with the International Organization of Standards (ISO).

Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA<sup>®</sup> Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor<sup>®</sup> (CISA<sup>®</sup>), Certified Information Security Manager<sup>®</sup> (CISM<sup>®</sup>), Certified in the Governance of Enterprise IT<sup>®</sup> (CGEIT<sup>®</sup>) and Certified in Risk and Information Systems Control<sup>™</sup> (CRISC<sup>™</sup>) designations.

The IT Governance Institute<sup>®</sup> (ITGI<sup>®</sup>) is a nonprofit, independent research entity that provides guidance for the global business community on issues related to the governance of enterprise IT assets. ITGI was established by the nonprofit membership association ISACA in 1998.

## **Attachment A—Responses to Questions**

ISACA's responses to the cybersecurity discussion paper's questions are based on our review, and are included in italics for each of the questions.

### **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?

*There is a need for increased awareness that digital citizens are NOT anonymous on the Internet and they are responsible for the consequences of their actions. Cybersecurity education needs a central agency to take the lead, coordinate and foster best practice. This includes protocols on behavior. Accepted behavioral protocols should be established through international agreements/mutual recognition of laws and enforcement across jurisdictions.*

*Guidelines for Australian online ethics, rights and responsibilities should be developed through a broad public discussion including individuals, business users, online service providers, professional organizations with cyberfocus, as well as all three levels of government. As it is unlikely that this input will be provided from key categories of stakeholders at this early stage, it is critical that the first and second iteration draft go through a public forum, through independent NFP professional bodies, such as ISACA and the Australian Computer Society (ACS), consumer protection groups and the media. This would assist with obtaining a broad consensus, which is essential and would help with promoting a concept of digital citizenship and acceptable behavior and user responsibilities. It is also critical that this agreement be delivered in the form of guidelines, rather than legislation, due to internationalism and the perception of anonymity of Internet users.*

**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?

*Companies need to:*

- *Work to build a culture of security. ISACA has produced a practical research deliverable (Creating a Culture of Security) addressing, among other things, how to institutionalize and sustain the intentional security culture.*
- *Be accountable for retaining the information necessary for the potential use of law enforcement*

- *Ensure that they are “good (online) corporate citizens” by acting upon complaints, tightening enforcement of conditions of use and ensuring they improve their own security controls, conditions of use, privacy settings, and requirements for account establishment and maintenance*

*Government strategy is required to make:*

- *Good online corporate governance more beneficial than costly*
- *Sites accountable in terms of security, privacy, and conditions of use, allowing for easier collection and analysis of evidence for prosecution*
- *A culture of security a required good practice for governments and companies*

*Once accepted by Australian community leaders, digital citizenship could be promoted via:*

- *Existing educational programs*
- *Being embedded in business-to-consumers (B2C), business-to-business (B2B), government-to-business (G2B) and government-to-citizens (G2C) services, such as Terms and Conditions acceptance of financial institutions and online service providers*
- *Independent NFPs, including professional associations such as ISACA and the ACS*

**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?

*This equally applies to seniors and other vulnerable people. Government should engage NFP sector experts to provide practical advice to parents through the media. This advice could also create opportunities for local businesses and stimulate the private sector to provide necessary services. For instance, government and experts from independent NFP professional bodies such as ISACA and ACS, but also consumer advocacy groups (e.g., Choice), could inform the public about PC vendors, operating systems, additional software packages and services, and ISP and mobile network providers that have tools to log online activities or block inappropriate content. Through promotion of this issue, education and empowerment of parents, and increased visibility of available products and services, the market is likely to respond and improve cybersafety of young people.*

*Illustrative Internet safety tips for parents (to complement the Guide to Online Safety – Cybersmart):*

1. *Discover the Internet together with the child.*
2. *Agree with the child on a framework for Internet use in the home.*
3. *Encourage the child to be careful when disclosing personal information.*
4. *Talk about the risks associated with meeting friends online.*
5. *Do not be too critical toward the child's exploration of the Internet.*
6. *Report online material that may be considered illegal to the appropriate authorities.*
7. *Encourage good netiquette.*
8. *Know the child's Internet use.*
9. *Remember that the positive aspects of the Internet outweigh the negatives.*

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

*Mandatory reporting of complaints by social networking sites/telcos/ISPs/schools could be considered or, if that is considered too restrictive, it should at least be made clear to whom complaints should be reported. For example, schools have a range of reporting obligations but only need to report to one authority for an investigation to occur; this same authority could be made responsible for initiating and coordinating the investigation kick-off for an online incident. A similar body to which “responsible” sites should report needs to be considered.*

*Ensure that schools/parents and police have the necessary means to act and enforce consequences where a bullying incident occurs online. A core issue of protection and what makes actions in the online world so difficult is the existing permanency of those online actions. A body that has the ability to regulate/enforce/influence across the major online players to limit consequences and permanency of the offensive post should be considered. It is critical that governments, the media and NFPs place sufficient pressure on main social networking platform providers to comply with the Digital Citizenship Guidelines.*

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?

*A majority of social media is provided by for-profit organizations, which are sensitive to public perception of their services, brands and impact on communities. Government, educators, social workers and experts from independent NFP professional bodies (ISACA, ACS, etc.) can directly encourage service providers to voluntarily implement safeguards supporting Digital Citizenship Guidelines.*

*It is essential that law enforcement agencies create multilateral agreements that enable prevention of cross-border online criminal activities. Perhaps successful international collaboration implemented to eliminate online child pornography could be extended for other types of activities that are universally accepted as illegal (e.g., malicious software distribution).*

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?

*Australian federal, state and local governments have had limited success in using social media to engage and mobilize businesses and individuals to improve social well-being. Examples of governments, with the assistance of academia and NFPs, successfully using social media are:*

- *Iceland's online constitution*
- *Swiss model of direct democracy*
- *US White House online petition initiative that promises an official response to any petition with more than 25,000 signatures*

*In addition to policy making, health services, education and social inclusion services could be major beneficiaries of social networking-based services. For instance, the elderly could provide online tutoring to schoolchildren no matter where they are located. NFPs, businesses and government could also sponsor awards for innovative social media services, which when combined with the National Broadband Network (NBN) could create the right climate for delivery of innovative online services.*

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

*Authenticity and integrity are pervasive issues in an online environment and are further emphasized when there is no immediate benefit of the transaction. Online fundraising should either be regulated externally or self-regulated with a trusted independent party providing a mechanism for digital citizens to validate fundraising activities. Potentially, the Australian Tax Office could assist in this process by having an online register of organizations whose fundraising efforts have a tax-deductible status.*

*Any use of the Internet comes with inherent risks to security that cannot be fully controlled; however, there is a range of controls that are well established to minimize such risks. Operators need to be held accountable if they do not meet generally accepted standards and, again, enforcement needs to occur.*

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?

*The government should require all organizations to protect not only the organization's interests, but also to mitigate the risks to all stakeholders from information security failures resulting from inadequate controls.*

*Governments should ensure they have access to the appropriate expertise and that risk management systems are in place to protect information from citizens and businesses. Classification markings signifying private information should be considered.*

## **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?

*Baseline requirements need to be made available, along with penalties for the providers and those who act as their own providers. This will ensure better protection, fewer breaches, and severe penalties if corners are cut and lessen the extent or consequence of breaches.*

*Government should engage cyberexperts through their professional associations to reach out to business education providers and cover relevant online risks and obligations, such as PCI DSS compliance, privacy obligations, securing online presence (e.g., particularly in the light of the recent Distribute IT breach). Cybersecurity must be considered an essential business skill. Therefore, small business education programs should be created to empower small business owners to better manage online risks by creating secure processes and implementing appropriate cybersecurity systems that are already widely available on the market.*

*As part of an awareness-raising campaign targeted at business, key messages should state the need for a workforce that is:*

- *Aware of the security risks*
- *Aware of their responsibilities to act in a responsible and secure way*
- *Applying the policies and best practices adopted by the business*
- *Responsive and proactive with the reporting of security incidents*
- *Mindful and understanding of their legal responsibilities toward information security*

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

*As an example, maintain the onus to cover fraudulent transactions and to protect the consumer with the banks and credit providers, but add fees and charges or fines. They will improve self-regulation and regulate businesses using their services if they are financially and legally accountable for what happens to the consumer.*

*Businesses could display their acceptance of Australian Digital Citizenship Guidelines or a suitable voluntary code that could be used to improve confidence in e-commerce transactions processed by those providers.*

*Education and awareness related to the Australian Digital Citizenship Guidelines and increased professionalism in cyberroles, supported by education sector and NFPs, would further improve consumer confidence.*

*Improved coordination between ISPs, online service providers, financial institutions and government (consumer protection and law enforcement agencies) would also improve overall safety and confidence.*

*Government and NFPs should identify areas that would be regulated by the industry (e.g., IP piracy) and focus their efforts on areas that do not have commercial drivers in the industry (e.g., privacy, online scams). To address these areas, government organizations such as CERT Australia may need to expand their role beyond current focus on critical infrastructure and national security.*

*Introduction of mandatory reporting of security breaches would likely increase overall security capability and maturity in the mid-term and increase overall consumer confidence in e-commerce.*

**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?

*Government should utilize the strong interests of the private sector to build and maintain confidence in the digital economy and improve user awareness of cyberrisks. Governments and NFPs should promote the importance of cybersecurity of online services to stimulate business to embrace it as a competitive advantage. However, it is essential that these activities be performed in cooperation with the private sector to ensure that competitiveness does not stifle cooperation in cybersecurity capability development, intelligence sharing and security awareness development.*

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

*Make it clear to whom data breaches are to be reported (particularly by a consumer or citizen) and make it easy to do. Where a breach involves private consumer/constituent information or financial data that may impact someone, reporting should be mandatory by the custodian of the information.*

**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?

*The reporting body can deidentify and distribute reports, creating a potential decrease in online fraud for banks and merchants.*

*Governments could stimulate a partnership between e-business and consumer protection groups to create an independent, self-governed feedback system. This system would need to rely on voluntary adoption to avoid industry backlash. However, the feedback system is in the interest of the entire sector and is even more valuable for e-business if it is obviously independent. One of the ways is to create an open standard, feedback exchange mechanism and application*

*programming interfaces (APIs) resulting in a platform that can utilize existing product, retailer and service feedback platforms.*

**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?

*To minimize cybercrime, bullying and poor security over personal and financial information, etc., there should be clearly defined and enforced penalties. Policing and consumer protection need to focus more effectively in these areas, which will require resourcing and cross-jurisdictional cooperation for investigating through multiple layers (ISP, telco carrier, vendor, site, etc.).*

*The possibility of extending consumer protection via multilateral agreements would be welcomed by Australian consumers and businesses considering offering services globally. In relation to more significant online scams and frauds such as investment scams, consumers expect timely warnings in the media and having these fraudulent e-mails being blocked or delivered with a scam warning. It is reasonable to expect that once a serious investment scam is reported and validated as fraudulent, no other users should be able to receive the message. Existing losses suffered by Australians are significant enough to warrant investment in a comprehensive protection scheme. Consideration needs to be given to what agency could play a role by coordinating this effort among ISPs and by issuing cybersecurity alerts on an opt-in basis, similar to the existing Smart Traveler bulletins.*

**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?

*Comparatively high e-commerce adoption in Australia indicates that consumers have trust in conducting business online. The other consumer protection and cybersecurity education measures discussed in previous questions would maintain this trust for existing online business users and possibly assure a portion of users currently abstaining from e-commerce. For instance, NFP consumer protection groups could promote services that provide insurance for e-commerce transactions, such as PayPal.*

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

*An explanation and justification of why personal information is required across government, physical business, banking and finance, and online should be required. The mandate that this*

*information needs to be provided to any third party should include from under whose authority is it requested (the Australian government or consumer protection organization) and who is responsible for its protection, consistent with existing privacy legislation and standards.*

*Australian Digital Citizenship could further clarify rights and responsibilities, as long as the information is delivered in an appropriate format to include broad demographics. Government and NFPs should develop wide-ranging education programs to inform consumers about their responsibility to protect their information and what types of services are high-risk.*

**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?

*There must be consistent application of accountability and enforcement where due care has not been taken.*

*Greater transparency over existing controls that are in place (where this does not jeopardize controls) would result in increased consumer confidence. For instance, banks following up unusual transactions with customers assist in building consumer confidence. Promotion of cybersecurity credentials, such as existence of ISO 27001 information security management system, and acceptance of voluntary codes, like Australian Digital (Corporate) Citizenship Guidelines, could further assist in building trust and confidence.*

*The industry should also increase transparency over the ways private data are used. Privacy commissioners and NFPs should maintain a healthy pressure on the industry to maintain consumer privacy.*

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

*Education, training and awareness campaigns should provide organizations options for improving cyberprotection of intellectual property, customer data, services and critical infrastructures as well as the development of improved cybersecurity tools and practices.*

*Timely information about threats, incidents and practical cybersecurity behaviors and controls should be accessible to consumers and small business. For instance, information about compromised web sites and services would be useful. Furthermore, everyone whose personal or business details have been compromised should be notified and provided with advice to improve their security, such as changing passwords and security questions on other online services. A government body should be made responsible to facilitate these small business and consumer cybersecurity protection and educational activities.*

*A technically skilled and cybersavvy workforce is critical.*

**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?

*In comparison to other utility service providers, such as power and water suppliers (which provide information about energy and water savings, etc.), ISPs provide little information to their users about securing their online experience. ISPs should take a more active role in educating users and providing at least basic firewall protection and content and spam filtering facilities that can be managed by the user. They should be able to provide activity logging in the same way phone calls are logged.*

*In terms of hardware, consumers expect to have basic security services included in the product. On the other hand, vendors and retailers see security products as another revenue stream, rather than an essential feature. For instance, it should be unacceptable to sell computers to consumers without a preinstalled, fully supported antivirus and firewall software (instead of a time-limited trial), especially when the operating system provides these facilities out of the box or as a free add-on.*

*An industry code of practice and cyberstandards could improve this position and flag compliant providers and vendors. Government, experts from independent NFP professional bodies such as ISACA and ACS, and consumer advocacy groups (e.g., Choice), could inform the public about the importance of cybersecurity and identify products and services that do not comply with these codes of practice and cyberstandards.*

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

*A central agency could take the lead for:*

- *Communicating protection strategies and information on how these can be implemented in practice*
- *Promulgating and monitoring appropriate security-related controls for organizations*
- *Creating and maintaining a minimum security standard set*
- *Creating a safe and confidential intelligence exchange network for businesses*
- *Introducing a voluntary security domain allowing consumers and businesses to access secure services (e.g., for financial transactions) if they implement required security controls and block “dark corners” of the Internet*
- *Cooperating to investigate and enforce using sufficient resources and penalties. It should be made very clear that there will be consequences for criminal activity online in this country.*

**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 AFP estimates 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?

*The botnet example provided in the discussion paper, while valid, is likely not the root cause of the majority of loss from cybercrime. The greater loss likely is associated with denial of service*

*(DoS) or other attacks luring individuals to a criminal site. Subject to this clarification, the forms of malicious activity these infected computers are used for should still have actions developed to defend against them and a plan created to deal with the perpetrators.*

*ISPs/telecommunication companies should have the responsibility to immediately cut connections of infected computers where known attack traffic is detected or reported and subsequently passed on to them with a known IP. This also reinforces the requirement for the ISP to keep logs to identify from which account the infected machine communicated.*

*The ISP should undertake proactive monitoring and block malicious traffic from within the ranges allocated to consumers. To be protected legally, the ISP should further be required to drop and report traffic matching infection patterns to the consumer.*

*Assistance would be required from a government/regulatory mechanism to implement the protection, assign responsibility and select the criteria needed to determine an infected computer to be dropped (e.g., a variety of online vendors and security sources monitor traffic and virus reports globally; a central government body could monitor, consolidate, analyze and report back). Carriers should be responsible for monitoring their networks for any malicious activity and responding accordingly.*

*Government should regulate cybersecurity baselines for online businesses and step in after each reportable major breach and assure the public that the provider is fit to provide secure online services (in a similar manner to how the Japanese government delayed the Sony Playstation<sup>®</sup> Network until it was assured it is safe for consumers).*

**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 wellbeing of the Australian community?

*Government should formally engage cybersecurity and social studies experts in the creation of the Australian Digital Citizenship Guidelines to articulate practical roles and responsibilities of stakeholders in the online environment. Government could take the role of coordinating these activities through a support network comprised of government, NFPs and private sector cybersecurity professionals. Through an agile, open and cost-effective exchange of security intelligence and coordination of cybersecurity prevention and incident response activities, Australia could significantly increase its security posture. This could make Australia an unattractive target for cybercriminals.*

*Software vendors should ensure out-of-the-box security and updates automatically applied, etc., while settings can be modified. This will address the majority of the issue from the average user.*

**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?

*Make it clear and easy as to how to report and to whom. For example, a person who was recently scammed could not find a single agency who would take the report. While it may take some time to sort out jurisdictional issues, there should still be a single, agreed point for a report to be made. Reviewing the “Stay Safe Online” booklet demonstrates how completely uncoordinated the present system is, especially where it involves a need to report to police.*

*Demonstrating that government responds toughly and swiftly on electronic crime will make victims more inclined to report incidents. Government should use cybersecurity experts, psychologists and social workers to further analyze and refine these principles. Once the right approach is agreed upon, these principles should be widely advertised much like the Crime Stoppers schemes.*

*Law enforcement agencies must be appropriately equipped, skilled and trained, as currently reporting a cybercrime is cumbersome even for cybersecurity professionals, let alone the general public (e.g., in some jurisdictions it is possible to report a car accident online, but it sometimes takes talking to several officers to find one who is willing to record a reported e-crime. Even those officers would admit that they do not know how this report is going to be handled.).*

**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?

*There is clearly a need for a network of government and law enforcement agencies, NFPs, insurance organizations, financial institutions and other businesses to exchange available security breach information in a secure environment and to encourage the public to report actual or attempted cybercrimes.*

**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 transactions 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?

*Lack of resources for online security should not take precedence over protection of the consumer. Government-funded or -subsidized payment gateways (possibly run by financial institutions) could be considered. Regardless, clear and mandatory security baselines must be established and penalties for breaches enforced (e.g., credit card numbers are prohibited from being retained on publicly accessible databases; independent audit and certification of sites are required, etc.). Regardless, “e-business in a box” needs to be stopped and people with appropriate skills used for set up. Penalties need to surpass the savings from not setting up e-business security properly.*

*Government small business training programs should include cybersecurity modules created and presented by security professionals and then provide an ongoing cybersecurity advisory jointly with financial institutions. ISPs should also provide basic cybersecurity advice as part of the service. The ISPs could be incentivized by an opportunity to generate additional revenue through secure services, such as Secure DNS, encrypted online data backups and web application vulnerability assessments for hosted web applications and sites.*

### **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?

*It is important that individuals be made aware of their role in national cybersecurity. This message needs to be delivered broadly and in an appropriate format, through a variety of outlets, including an awareness campaign, public service announcements, NFP conferences (such as those held by ISACA), business roundtables, the Internet, and other media channels. The public pays attention to real-life crime stories, especially when individuals can relate to them, evident by the success of Border Control and RBT television shows. It is possible that cybercrimes would spark a similar interest. Providing more prominent media coverage (similar to other law enforcement reality shows) could improve public understanding of interdependencies between individual and national cybersecurity. Furthermore, ISPs need to assist their customers to improve their cybersecurity posture.*

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

*By taking preventive actions based on much greater awareness than currently exists; hence, more communication to the community on the issues and risks currently faced is urgently needed. Awareness and the issues highlighted in this response with respect to business, government and (software/security) vendor responsibility to ensure security at their end is also needed. Basic guides for people less used to technical security threats, such as those contained in the Attorney General's guide from Cyber Security Week, and general awareness raising like this are a very good start. Technically skilled and a cybersavvy workforce would also help in increasing protection levels. A rigorous certification system should be set up and publicized.*

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

*No, individuals are not adequately aware of cybersecurity threats. For the most part, they believe they are purchasing through legitimate, trusted software and hardware vendors and are setting up their systems according to instructions. However, cybersecurity is a complex discipline. Therefore, it is unreasonable to expect individuals to be fully aware of cyberthreats in a complex and dynamic environment, which is clearly asymmetric. This is why governments, the industry (particularly financial institutions and ISPs) and independent NFP professional bodies such as ISACA and ACS need to assist individuals and provide them with baseline security by default and with simple and timely security advice.*

### **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?

*Considering internationalism, the perception of anonymity of Internet users, and the infeasibility of effective and widely acceptable Internet filtering, Internet governance must be based on a collaboration of ISPs, online service providers, governments, media, NFPs and the public, all working toward the development and sharing of a clear set of defined standards. Current legislation should also be updated to address online felonies and criminal activities.*

**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?

*Consultation such as this paper is an excellent start. Careful balancing among security, convenience and risk taking is always required. Market forces are likely to provide the right balance in commercial areas; however, the government and NFPs have a role in securing privacy and ethical use of data and cyberresources by engaging in a broad debate and gradual implementation of suitable guidelines and regulations.*

*Also, the governance model applied to an Australian-based Internet presence must ensure that all businesses dealing with consumer information maintain minimum security standards. This can assist with the country's online vendors being seen as safe, secure locations to conduct commerce.*

**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?

*A consultative approach should be taken with a view to protecting users. Governments need to work together to influence providers to ensure secure and safe sites, with clear and enforced conditions of use to protect users from both crime and inappropriate behavior. The only bodies that can adequately monitor and control inappropriate behavior on the major social networking sites are the sites themselves. However, they can be influenced as to what the government considers “good” corporate citizenship on the Internet, through laws governing collection, retention and provision of logs across all the components aggregating the connection from home to the Internet. Agreements between Australia and major governmental partners (e.g., USA, UK) on what constitutes appropriate behaviors should be able to be reached due to the similarities in cultures, values and consumer protection views to align sites operating from any of these jurisdictions.*

### **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 cyberworkers 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 discussion paper places strong emphasis on cybersecurity as a pillar of Australian cyberfuture. However, it does not address a widespread shortage of suitably skilled, experienced and certified cybersecurity professionals in private, public and NFP sectors. This scarcity is more significant than the general cyberskills shortage outlined in the paper. Organizations are often faced with a choice among bringing in resources from overseas, assigning unsuitably skilled resources or leaving cybersecurity roles vacant. This is happening at a time when cybercrime is thriving and when business interdependencies, outsourcing and cloud computing are further increasing risks and increasing the demand for cybersecurity professionals. Therefore, building Australia’s cybersecurity capability and capacity should be a priority that will require a cooperation of independent NFP professional bodies (such as ISACA), tertiary education providers and the government.*

*The ISACA designation [Certified Information Security Manager](#)<sup>®</sup> (CISM<sup>®</sup>) is focused on skills important for good cybersecurity prevention. The domains of CISM provide the basis for the ISACA [Model Curriculum for Information Security Management](#).*

*Only after building this core workforce of cybersecurity specialists will Australia have the capability to propagate these skills to other cyberprofessionals and the public. Other things to consider include a mixture of education and training within the country, ranging from apprenticeships for “learning by doing” tasks, to roles focusing on simple tasks (e.g., basic networking with CCNA being achieved in school and the person going straight into the workforce), through to university education.*

*Promotion of professionalism within cyberprofessions (through qualifications, professional membership and certifications) and support for creation of entry-level cyber and security roles would improve domestic expertise. Experienced cyberresources in the areas that are declining could also be retrained to become cybertraining and cybersecurity professionals. Governments can have a significant impact indirectly, by insisting that internal cyberresources and engaged contractors and consultants hold adequate cyberqualifications and certifications.*

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

*Building a competent workforce incorporates three complementary components: workforce planning, professional development, and the identification of core professional competencies. Workforce planning analyzes the functional capabilities needed to achieve the current mission, forecast future capabilities, and identify specific knowledge, skills and abilities for cybersecurity professionals. Education and independent NFP professional certification providers, such as ISACA and ACS Education, could promote cybersecurity education and certification programs beyond security professionals to include broader members of the public. School systems should continue to have cybersecurity as a crucial part of cyberstudies. To support wider adoption of cybersecurity professionalism, government could insist on suitably educated and certified professionals for key cyberroles. This could also extend to businesses and contractors providing services to government. All positions of trust should have appropriate cybersecurity skills and credentials. Government could stimulate creation of more entry-level cyberroles and identify entry roles for graduate cybersecurity professionals, as these have been steadily declining, partially due to offshoring and other industry trends.*

**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?

*Continue with existing government education, communication, outreach to media, and public awareness services such as Australian Securities and Investment Commission for fraud. Identify a single authority or body to be responsible for cybersecurity, act as the conduit to the community, and serve as a single site/contact number for people to refer to (as discussed earlier in this document) for all such matters/awareness/scam reporting.*

*The government could engage professionals and independent NFP professional bodies to create accessible education programs for the community. Government—with assistance of professional cybersecurity NFP professional associations, such as ISACA and ACS—could help reach out to the current community education infrastructure (e.g., libraries, community and religious associations) and train them to deliver these key community messages.*

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?

*Trust is a clear differentiator between Australia as a digital economy and the remainder of the world that can be directly influenced by government and industry here. The points raised in this response promoting government intervention have all pertained to accountability of the online shop/vendor, etc., to ensure they have taken every reasonable step, including meeting minimum standards or suffering penalties, to ensure the security of their sites and their customers' personal and financial information. If Australian based e-commerce initiatives are seen to be the most reliable and trusted in the world, resulting from government regulations and subsequent performance, then they can be seen as a preferred trading partner. If Australia is seen as an example of global best practices, then digital investment will follow.*

*However, to demonstrate government support for digital investment, government should make significant improvements to G2B and G2C services. For instance, tendering and procurement processes could be simplified and made more online-friendly.*