The Australian Computer Society

Response to

The Department of the Prime Minister and Cabinet's Discussion Paper

"Connecting with Confidence"

November 2011

Preamble

The Australian Computer Society (ACS) is the recognised association for Information and Communications Technology (ICT) professionals, attracting a large and active membership from all levels of the Australian ICT industry. A member of the Australian Council of Professions and active member of the International Federation for Information Processing (IFIP) under the auspices of UNESCO, the ACS is the public voice of the Australian ICT profession and the guardian of professional ethics and standards in the ICT industry, with a commitment to the wider community to ensure the beneficial development and use of ICT.

In fulfilling our role, the ACS is active on a range of policy fronts and among ICT stakeholders to improve ICT skills, education and training capability and quality in Australia and to promote the responsible and professional use of ICT as it affects almost every aspect of daily life. The ACS supports the development of Australian ICT and works with key stakeholders to provide annual ICT reporting as well as to explore ways to further improve the measurement of ICT's contribution to the economy, community and the environment so that we can make informed policy decisions. These policy areas have informed our response to the discussion paper.

Introduction

Developed nations have long recognised the need for a coordinated international policy response to our increasing use of and reliance on online systems, and the severity of cyber risks which ignore borders and jurisdictions.[1] However, despite this ongoing recognition, a coordinated policy response is still to emerge. For example, as far back as 2002 the Computing Research Association [2] detailed four key challenges to defining technical and social challenges in trustworthy computing which were then provided to the US Congress. These were:

1. Within the decade eliminate the threat of all epidemic-style attacks such as viruses and worms, spam, and denial-of-service attacks.
2. As many new systems with great societal impact are currently planned or under development, develop tools and design principles that will allow these systems to be highly trustworthy.
3. Develop and validate quantitative models of risk and reward and deploy them to decision-makers so that progress can be made.
4. Lastly, setting its sights on the dynamic, pervasive computing environments of the future, provide understandable and affordable security and privacy to tens of millions of new users.

Since 2002 our online world has dramatically changed. In 2003 Facebook was still in University dorms, Twitter did not exist and malware and cyber-threats amounted to a fraction of what they are today. But almost a decade later these threats are even more pressing, and indicate the need for governments worldwide to take real interest in the safety and security of "cyberspace" beyond responding to attacks.

ACS members design, implement, and maintain the online systems which underpin the Australian economy for the benefit of the Australian community. The ACS has a vital interest in seeing that these systems are secure and in ensuring the proposed 2012 whitepaper details real policy guidance directed at national ICT research organisations to address these challenges as they are critical to meet any objectives that the whitepaper may have. We suggest that *Moving from Trusted to Trustworthy* would be an appropriate theme to complement the *Connecting with Confidence* discussion paper.

The ACS has prepared this response to the discussion paper to assist with the design of the cyber whitepaper expected in 2012. The ACS also welcomes the opportunity to promote discussion and support of our digital economy to position Australia for the future. Drawing from its membership of ICT professionals, and academics – particularly in areas of cyber resilience and security - the ACS established a Cyber Taskforce for this purpose.

While the ACS Taskforce will respond in broad terms to the issues raised by the discussion paper, the Taskforce also appreciates the opportunity to highlight important issues not fully articulated in the paper and hopes that these will help to inform future discussion and policy leadership.

The ACS recommends

- greater focus on education - noting that ICT education in primary and secondary schooling is essential to developing ICT skills of the future and that school level educational activity forms the base on which appropriate tertiary level education programs can function for the education and training of ICT professionals
- greater assistance to small and medium sized business as this is the engine room of the Australian economy [3]
- policy coordination on trusted identities
- better coordination of cyber related education and research
- providing consumers and businesses with resources directed to the everyday real-life challenges they face
- global Internet governance changes designed to underpin and deliver trustworthy people, processes and systems including, where appropriate, a legislated mandatory baseline of trustworthiness attributes analogous to the non-excludable warranties implied in consumer contacts.

In addition, many critical contingencies for Australia to 'connect with confidence' are absent in the discussion paper. Most notable are issues of cyber space sovereignty, such as Free Trade Agreements, the rights of individuals, privacy leakages and breach notification reporting, freedom of information and the role of data collection agencies. As ICT is a truly global profession and operates in global markets, the whitepaper should recognise this basic fact. In particular, the roles and responsibilities of the ICT industry, and its vendors and system operators, must be emphasized so that professionalism becomes a fundamental element in achieving trustworthiness in people, processes and systems.

The discussion paper is a welcome multi-stakeholder approach and the ACS recommends the whitepaper continue this focus. Government cannot 'connect with confidence' alone and neither will a sole focus on the end user who remains a convenient target to apportion blame for cyber issues. Following US congressional hearings on cyber threats this year, former General, National Security Agency Chief and CIA Director, Michael Hayden, explained that:

> *"Some have observed that the free market has failed to provide an adequate level of security for the net since the true costs of insecurity are hidden or not understood. I agree."* [4]

Many organisations in both the public and private sector have demonstrated improvement opportunities in ensuring the security of IT and information as vital in supporting the infrastructure for the Australian economy and society as a whole. There are many sensitive categories of information [5] and it is therefore essential that all organisations be subjected to regulatory requirements, including specific security standards, and both civil and criminal sanctions for breaches of those standards.

In this respect the ACS emphasises that it is also important for governments and regulators to undertake Regulatory Impact Assessments (RIA) to evaluate the potential regulatory burden on businesses. An RIA helps to ensure that proposed regulatory measures are proportionate to the risks in the target policy area, transparent and consistent in their operation, and minimise the impacts on the industry, particularly small and medium size enterprises (SMEs) which otherwise could potentially decrease competitiveness. In other words, the whitepaper needs to guide stakeholders on how to achieve balance between the need for robust regulation and avoiding unnecessary restrictions on businesses.

Clear Objectives, Risks and Treatments

As with other OECD member policy responses [6] to the challenges of the digital age, the whitepaper would benefit from identifying clear measurable objectives beyond the aspirational "connecting with confidence" statement and would benefit with clearer reference to the national digital economy strategy. [7]

It is recommended the whitepaper adopts a risk management approach to ICT so risk can be accurately measured and addressed. [8] In this respect the ACS notes that *treatments* for risks – such as legislation, policy, education, or certification - should be used in preference to the discussion paper focusing on risk *mitigation*.

The discussion paper understates the risks of an online Australia and it is suggested the whitepaper expands on risks and benefits. As an example of understating risk, the discussion paper claims that Wikipedia has not only made knowledge more accessible but that *"it has also democratised the creation of knowledge."* However, whilst popular, Wikipedia's disclaimer [9] clearly states that while the information in Wikipedia may be *democratic* it may not be reliable. More pertinently, Wikipedia has been linked to malware.[10] The whitepaper should carefully consider the examples it chooses in promoting its aims, acknowledging that threat assessment is not static as windows of vulnerability evolve over time.

The ACS supports the provision of online services and notes the benefits detailed in the discussion paper – particularly in relation to online government service delivery - and encourages the whitepaper to also describe in detail the risks to inclusion and participation associated with this trend. For example, the discussion paper does not describe the potential to disenfranchise digitally illiterate populations such as low income earners and the elderly. Nor does it describe the potential for businesses and government agencies to encourage migration to (cheaper) online customer service portals by purposely reducing other lines of available service via, for example, increased average waiting times to customer helplines or reduced customer facing staff in regional Australia. These audiences, as noted previously by the ACS, form a new 'digital divide' regardless of their geography. [11] In this respect the whitepaper could similarly describe the risks to privacy and controls on data usage in relation to benefits described in the National E-health strategy, also highlighted in the discussion paper.

Defining and measuring our Digital Economy

The whitepaper could also benefit in describing the Australian ICT ecosystem, recognising that a significant difficulty in understanding the ICT landscape is the frequent confusion between analysis of the ICT work-force in labour market terms (e.g. what job the individual performs), and analysing the ICT work-force in Industry terms (e.g. what kind of organisation the individual worked for). ICT is evident in every industry sector just as it is pervasive in almost every aspect of our lives. Unfortunately ICT is not yet recognised as a sector in its own right and will remain so until the current metrics used in Australia based on ANZSCO/ANZSIC codes are updated to reflect the reality of Australian ICT in the 21st century.

ANZSCO (Australia, New Zealand Standard Classification of Occupations) is a multi-level nomenclature essential to the understanding of employment statistics. The upper level (the 2-digit level) is meant to group like occupations by their main grouping. Unfortunately, grouping ICT at this level leaves out some occupations that others would consider belong wholly or in part within ICT. Accordingly, simple extracts from employment data of the "ICT" ANZSCO group can easily lead to inadvertent understatement of the actual position of ICT employment.

ANZSIC (Australia, New Zealand Standard Industry Classification), is similarly structured to ANZSCO, and whilst it does have an upper level ICT grouping (Information Media and Telecommunications) which includes some small non-ICT elements, it unfortunately does not include the numerically larger Software and Services ICT industry sector, which is included as a misnamed sub-set (Computer Systems Design) within the upper level grouping "Professional, Scientific and Technical services."

"Information Media and Telecommunications" also leaves out the ICT hardware manufacture, ICT wholesale and retail trade, and ICT consulting sectors, which are scattered across a number of other ANZSIC groups.

General economists and other commentators sometimes presume that "Information Media and Telecommunications," in ABS data and government publications, is the ICT industry, and make comment without realising that in employment terms, it is actually less than half of the employment in the "real" ICT industry. This same analysis impacts upon calculations of ICT revenue, exports, and Gross Value Added / Gross Domestic Product (GDP/GVA), which regularly become a synonym for economic importance and are

frequently understated for ICT but overstated for the industry sectors in which the missing ICT industry sectors are hidden.

The ACS submits that a more appropriate classification of ICT occupations is required to understand the ICT sector and the "digital economy' in Australia and thus inform ICT policy with a clear, verifiable set of metrics, potentially by reference to the Skills For the Information Age (SFIA)[12] framework. The ACS maintains that the SFIA framework is the preferred model for referencing the skills needed to develop effective information systems as it is based on competencies rather than solely on qualifications. SFIA has been adopted by the Australian Government Information Office (AGIMO) to assist ICT skills mapping in the Australian Public Service. SFIA also underpins the ACS Framework for Professionalism endorsed by the Federal Innovation Council.[13]

The ACS supports the SFIA framework because it provides a standardised view of the skills needed by people working in Information Technology. SFIA describes required capabilities rather than technologically orientated knowledge of, for example, a specific system or application. Organisations that combine the SFIA skills with information about behavioural competencies and knowledge of relevant technologies and products produce highly effective professional profiles and job descriptions which form the basis for the management and deployment of IT capability.

The Australian Bureau of Statistics (ABS) has measured the ICT Industry intermittently as a specific exercise since 1996, with its last report now over five years old representing the period 2006-7 (cat 8126.0) and published in October 2008. This report was referenced for the ICT industry data in the 2009 ACS ICT Statistical Compendium.

Since 1998, the Centre for Innovative Industries Economic Research Inc. (CIIER) has conducted an annual survey on a smaller survey sample, modelling the ICT industry in a similar manner to ABS. The ICT industry data for the ACS 2011 Statistical Compendium draws upon CIIER's December 2010 data as well as other ABS statistical data and information.

Further confusion can also arise with the use of the terms "Digital Economy" and "Internet Economy" to describe elements of the economic processes of all industries impacted by ICT, or by the specifics of internet based ICT, and in some cases the productive elements (labour, infrastructure etc.) that make these possible.

It is easier to accurately define Australia's Digital Economy by what it is not, rather than by what it is. In the broadest sense it is almost the entire domestic economy, other than those very small components of the economy that do not use any ICT support at all (e.g. subsistence farming or street musicians - unless they also distribute their outputs electronically). More logically, it is all of the ICT industry, and a significant proportion of almost every other economic sector that uses ICT. Mining, healthcare, education, government, wholesale and retail trade, manufacturing, transport, and other sectors all rely on ICT goods and services, and are therefore participants in the digital economy.

The whitepaper could consider the Internet economy as defined as a varying subset of the digital economy potentially by reference to Treasury data. The variation is because the decision whether to use internet based ICT or internal organisational ICT is one that is made for lots of different reasons - technical, financial, data security or operational control - and those decisions change over time. The distinction is also economically irrelevant, other than for ICT suppliers whose markets are internet focused products and services. Unfortunately, these terms are used interchangeably, and the more narrow definition of "internet economy" may therefore lead to conservative interpretations of the significance of the Digital economy, and thus of the ICT industry and ICT profession that creates and maintains it.

The term "ICT Industry" is also often used for a confusing range of different things, ranging from the "tight" definition of companies solely concerned with the provision of ICT products and services, but which includes companies with major units supplying ICT goods and services, through a "looser" definition that may include retail ICT, that may include call centres that are mainly parts of other industries (e.g. banking), that may include significant sections of the electronics industries, and of other professional services (e.g. management consultants and, historically, accountants), to a "broad" definition that can include anyone working on ICT related matters in any industry.

This consideration is especially pertinent for the whitepaper to acknowledge the skills Australia will need to ensure the investment in the National Broadband Network is maximised and that there is an appropriate domestic workforce supply to address the online confidence issues which will only increase with greater online activity. Most acutely, the move to cloud computing has the potential to deliver substantial productivity and efficiency gains but only where the consequent risks are identified, managed and fairly allocated. At the moment the immaturity of the space leads to supplier imposed terms that divest risk onto mostly unsuspecting users. The analogy of unregulated "buyer beware" behaviour which led in the early 20th century to mandatory consumer protection measures is a strong one.

According to ACS research [14] based upon a regressive analysis of correlations to Australian share market indices, (effectively a surrogate for future investment intentions) Australia faces an ongoing demand for ICT skills. While the ACS acknowledges that forward share market index positions will vary from those projected, basing analysis upon conservative economist indicators indicates that unless Australia tips into a minimum two-year recession, net demand for ICT technical and professional staff will continue to grow over the next three years with a net demand of 14,000 in 2012, and assuming an ASX close June 30 2012 of 5000 points, 21,000 in 2013.

It should also be noted that this data is about net change in the workforce. Notwithstanding any growth in net demand, replacements will also still need to be made for retirements, external migration, the expiring of temporary visas, and other ongoing reductions in the Australian ICT workforce.

The ACS maintains that it is highly doubtful that ICT skills demand can be met from current education sources, as despite a slight increase in domestic ICT enrolments in the last two years, the neglect of domestic ICT education for the previous ten years still has a long way to go to recover to necessary levels to support Australia's digital economy.

Who to trust?

Citizens trust their medical practitioners because they assume an appropriate level of qualification, credentials and experience. The same attitude generally applies to many other professions including Lawyers, Pilots, Police, Accountants, Engineers and Architects but it is yet to be fully embraced by government in the context of cyber security or, indeed, ICT more generally.

Beyond considerations of professionalism, unlike mechanical switching for example, the internet relies on data tables which are constantly changing so that "trust" in an online context today extends beyond individuals to things and entities: Can I trust that this website is actually my bank? Can I trust that the application I am using – such as mobile banking – is secure? And can I trust that the person using it is the right person?

The discussion paper acknowledges that *trusted identity* is central to the digital economy but does not discuss the concept of "privacy" with due prominence, occurring only once in the discussion paper and only in reference to trust and confidence rather than about privacy *per se*. Reflecting on the discussion paper's origins in the national security cabal, the whitepaper could recognise how the potential for negative privacy impacts and implications can arise from well-intentioned measures, and describe how to best assess proportionality, consultation, and mitigation measures.

IBM summarises the importance of identity in the digital age as

> *[…] a new focal point in today's global economy, in which trust in your identity and credentials – and those of others – is essential in a variety of daily transactions. You use your identity to connect with people, groups and organizations, both digitally and face-to-face. Each connection is founded on trust and shaped by the ongoing confidence placed in the systems which create and manage your identities.*[15]

The "trusted identity framework" will be essential in meeting the challenges raised in the discussion paper and the ACS hopes the whitepaper will recognise the role of the Australian Information Commissioner to shape

broader consultation to this end. A framework should also be developed from a standards view anticipating national and international inter-operability[16] across markets which also recognises that the concept of "identity" in the national information infrastructure is much wider than just consideration of the identity of any human user of a computer based system. The largest population of connected entities on the Internet, for example, will consist of specific automated products and systems - an "Internet of Things." The "name and address" of any connected entity must be verifiable and thus trustworthy so that, for example, an automated electricity power meter reading unit can be identified and any measurements read likewise be authenticated.

The partnerships mentioned in the discussion paper are vague and the ACS would encourage more explicit delegation of responsibility within government and to non-government agents (including consumers) while recognizing that ultimately the Commonwealth retains accountability to the people of Australia for the benefits and risks resulting from the National Broadband Network. Explicit accountability to promote effective cooperation was among the key recommendations of the recent United Nations Office on Drugs and Crime–International Telecommunication Union (UNODC–ITU) Asia-Pacific regional workshop on Fighting Cybercrime.[17]

Aside from the need for clear articulation of inter-agency cooperation in planning and responding to cyber security issues, cooperation is especially important when considering the (potentially overwhelming) amount of government and private information available to citizens in assessing risks and opportunities online. For example, the discussion paper website itself lists thirteen government resources for information about cyber safety and has introduced new branding elements distinct from the other sources.[18] While all of these resources are worthy, positive and valuable, it is unsurprising that when this level of decentralized guidance is then combined with an increasing plethora of private sector information – such as ICT vendor advisories - authority is diluted, the risk of confusion increases, and malicious targeting is made easier.

While there are many non-ICT parallels which show the tragic consequences of confusion in knowing what information sources to trust [19] the government has already recognised to some extent that complex policy responses to cyber security have contributed to an increased risk among Australians.[20] Many submissions to House of Representatives Inquiry into Cyber Crime (2010) also highlighted this issue and advocated a centralized single source of authority [21] or at least a more coordinated and consistent approach to government communication.

Improved or more explicit delegations would facilitate information and intelligence sharing between all parties and help to mitigate cyber-crime risks, particularly those cyber-crime activities that target critical infrastructure. However, thought would also need to be given to the allocation of responsibilities in connection with any such centralized single source of authority, to which crime types would be included within its remit, and whether it should be located within an existing policy, research or law enforcement agency.

There are also a plethora of authorities who receive inquiries and requests from consumers and businesses on online issues. This also means a plethora of regulations, funding and resourcing issues, user guidelines and authority branding. [22]

The discussion paper's consideration of international arrangements and governance can be more fully discussed in the whitepaper by way of reference to Australia's key international cyber stakeholders, including the Internet Corporation for Assigned Names and Numbers (ICANN), the Governmental Advisory Committee (which provides input to ICANN), the Internet Society (ISOC) who provide global leadership on internet standards and policy, the Internet Engineering Task Force (IETF) or the Internet Governance Forum (IGF) which support the United Nations in the mandate from the World Summit on the Information Society (WSIS) with regard to convening multi-stakeholder policy dialogue.

The ACS agrees that developed countries currently dominate global Internet policy but the disadvantages in those countries characterised in contrast as lacking a strong civil society or internet infrastructure and skills, will not be resolved through further centralization (for example, via the UN) as proposed by India, South Africa Brazil and others [23] and the ACS recommends the whitepaper acknowledge this by appropriately valuing the open model of decision-making that has made the Internet the spectacular global success it is today.

The ACS is also concerned that the integrity of internet governance and the domain name system (DNS) can be compromised by dominant international interests - and by registrars – but that international integrity issues extend beyond DNS considerations to include IP address allocation, port numbers and protocol specifications. The whitepaper could consider how Australia's leadership among international forums can reduce cyber-crime, consumer detriment, and trademark abuses (a key enabler of phishing) from the plethora of new domain names.

At home, the ACS recognises that cyber sovereignty controls can be expressed through legislation and through voluntary codes. In practice, voluntary codes can be ignored resulting in little or no control and so to really "connect with confidence" the whitepaper could further consider explicit obligations on organisations and government agencies in relation to security, backed by sanctions, up to and including criminal sanctions. ASIC's new ePayments Code is a good start but we believe will need to become mandatory so that fringe dwellers cannot stay outside the trustworthy regime.

The ACS believes that the current legal framework based on the *Privacy Act 1988* (Cth) is an inadequate instrument to encourage the protection of data and that there is much value in the whitepaper considering mandatory data breach notification laws. The concept of data breach notification laws was a good idea in 2002-03 to achieve transparency and enable the public to understand – and make decisions – about organisational security practices. However, almost a decade later, and after a string of very serious and far reaching data breaches[24], the need for such legislation has gone beyond a good idea to a need that is now abundantly apparent and in that respect the whitepaper should give appropriate consideration to the data notification law recommendations set out by the Australian Law Reform Commission[25] and how these could be practically implemented. For example, how does one report a data breach without compromising an individual's privacy?

Education and Research

The discussion paper includes a welcome focus on education and the ACS would support the whitepaper further acknowledging the value of ICT education not only in importantly raising awareness and confidence among consumers, but as a fundamental lever to maximise the NBN investment and propel the digital economy. There are two areas of education the ACS is interested to see considered by the whitepaper.

The first area is a general and ongoing education campaign for the public at large embedded in their actual use and practice of ICT. For example, it is increasingly common for Australians to engage online via a mobile device rather than a laptop or home PC and yet there is insufficient awareness about the security risks peculiar to mobile devices. The second area is a greater focus on ICT in schools, vocational education and training (VET) and higher education with particular reference to the national curriculum, which is not evident in the discussion paper.

For general awareness raising, the whitepaper would benefit in evaluating the effectiveness of existing government-driven cyber awareness programs collectively in their raising of awareness among all audiences identified in the discussion paper and where potential integration and alignment of these programs could occur. This should not be undertaken in isolation but considered alongside such awareness programs run by States and Territory government agencies and in schools, particularly harnessing new media (e.g. social networking sites) to reach a wider audience.

A key message from the House of Representatives Standing Committee on Communications (2010) inquiry was that a more integrated, coordinated and concerted effort by government agencies, industry and community organisations is required to combat the cyber-criminal activities that victimise individual end users and businesses, and can help to ensure the most effective cyber-crime prevention advice is provided to the community (e.g. campaigns to ensure that individual consumers and front-line police officers know where and how to obtain information on how to protect themselves in cyberspace). It is, therefore, important to include academic and subject-matter experts in the development and delivery of the community awareness and education strategy.

Ongoing review is also required to ensure that the community awareness and education initiatives are up-to-date and take account of the most recent cyber-crime trends and best practice initiatives.[26] Further consultation is also needed to determine the most appropriate agency to coordinate the provision of information to consumers.

Longer-term measures should include a greater focus on cyber security research, and educating and encouraging individual consumers (and businesses) to report incidents to law enforcement and other competent agencies [27] so that the Australian Government has a better understanding of the current and emerging cyber threats and is able to develop responses to neutralise cyber-crime opportunities before they arise while promoting trust and trustworthiness frameworks. By way of example only, it should be illegal to supply broadband connectivity means in Australia with default settings that leave users open to cyber intrusion and abuse. There is community acceptance of mandatory seat belts and air bags in motor vehicles. The ACS submits that the ICT equivalent is necessary to achieve the baseline people, process and system trustworthiness that must underpin any 'connecting with confidence' regime.

Just as consumers and small businesses can benefit from increased awareness of cyber safety issues, the rapidly evolving nature of risks to end users requires more than just advice to keep personal information offline and install an anti-virus program. The escalating complexities of the end-user online environment underscore the need for regular ongoing training programs for basic online security (including new cyber-crime trends) and the promotion of a culture of security for information systems and networks among customers and staff of Australian businesses.[28] Again, training programs should not be static as cyber threats evolve over time. For example, a 2011 whitepaper by McAfee describes how the latest generation malware can "self-heal, reinstalling from a hiding place after a system has been cleaned, extending the compromised system's shelf life for the attacker." [29]

Many organisations provide valuable cyber security training and the whitepaper could acknowledge the need for a consistent framework to evaluate these. For example, the ACS runs an "Information Security" elective in its Computer Professional Education Program which is aligned to the SFIA skill Information Security" at level 5. Other SFIA security related skills include Network control and Operation and Security Administration.

A greater focus on ICT in the national curriculum, in the view of the ACS, would achieve many of the objectives of the 2011 Digital Economy strategy itself, and underpins most of its success factors.

In April 2011 the Australian Council for Computers in Education (ACCE) proposed that given the value of ICT education beyond study and work, ICT should appear in the national curriculum in its own right, either within the framework of the ICT and Design and Technology Learning Area, or as a new area. [30]

The ACS suggests further that ICT is not just an enabling technology profoundly changing our world view, but has deep theoretical underpinnings deserving of increased academic study. The ACCE also noted that the Melbourne Declaration [31] also recognises the importance of ICT in supporting learning across the national curriculum.[32]

The ACS shares with ACCE concerns regarding ICT's position within the national curriculum particularly around ICT competence currently regarded as a General Capability.

The ACCE paper also contrasted the placement of ICT in the Australian curriculum with the European Qualification Framework which defines competence as 'the proven ability to use knowledge, skills and personal, social and/ or methodological abilities, in work or study situations and in professional and personal development'. [33]

This view of competency describes ICT as a much more important attribute in our digital age than as described within the current General Competency and more closely supports the conceptual basis for the SFIA framework as described above.

The importance of education in ICT cannot be overstated; however the need for Australia to invest further in ICT research and development (R&D) along with ICT tertiary education is just as pressing. Australian R&D at

2.2 per cent of GDP ranks 14th among OECD nations[34], as a proportion of the total domestic workforce engaged in R&D, Australia ranks 16th. [35] As the President of the Australian Academy of Science, Susan Cory also recently observed, Australia is ranked 20th of 30 nations for the number of university graduates emerging with a science or engineering degree.[36]

Recent developments in Australian ICT R&D show a mixed view of ICT as application driven and do not fully recognise how ICT underpins other disciplines or that it is a discipline in its own right. For example, Australia's own ICT centre of excellence, National ICT Australia (NICTA), has a strong focus on bio-informatics. The recently established IBM research centre at the University of Melbourne has a focus not on ICT, but on vertical applications of ICT. The whitepaper can rightly highlight these issues and draw attention to areas in which ICT can be better promoted.[37]

Can Australia connect with confidence by continuing to simply buy commercial off-the-shelf ICT created by others and then seek to apply that ICT to our unique circumstances? The ACS supports the ACCE recommendations to ICT's placement in the national curriculum and maintains that the key to Australia achieving the goals of the national digital economy strategy are not to create a generation skilled in the use of technology applications or hardware, but a generation who can create and innovate in technology itself.

Conclusion

The ACS appreciates the opportunity to comment on the "Connecting with Confidence" discussion paper and believes the discussion paper initiative is an important first step in a more fulsome consideration of the challenges Australia faces in this digital century.

The ACS looks forward to further engagement in the cyber whitepaper in 2012 and hopes that the whitepaper will go beyond the cyber confidence issues raised in the discussion paper to examine, and propose solutions to, the areas of concern raised in response by the ACS as fundamental enablers of the Digital Economy Strategy and fundamental underpinnings needed to support a regime in which citizens can truly 'connect with confidence'.

The ACS Cyber Taskforce Terms of Reference:

a. To contribute to the preparation of submission to the Public Discussion Paper "Connecting with Confidence, Optimising Australia's Digital Future"
b. To support in the consultation with members of their views and opinions of the Public Discussion Paper
c. To make recommendations to the ACS Policy Committee in the submission to the Public Discussion Paper

The ACS Cyber Taskforce comprised

Taskforce Chair: Dr. Nick Tate, Director, Research Data Storage Infrastructure (RDSI) Project, The University of Queensland and National Treasurer ACS, together with:

- Mr. Philip Argy B Com; LL.B. FACS, MAICD, Past President ACS, Deputy Chairman of the ACS Foundation, Chairman of the National ICT Industry Alliance (NICTIA) and National Chairman, eCommerce Committee, Law Council of Australia.
- Professor Emeritus William J (Bill) Caelli AO, FACS, FTICA, Sen MIEE, Hon CISM, Fellow ISC^2 Director International Information Security Consultants Pty Ltd.
- Dr. Raymond Choo, MACS (Snr) CP, Fulbright Scholar, Senior Lecturer at University of South Australia, and Visiting Researcher at ANU's ARC Centre of Excellence in Policing and Security.
- Dr. Roger Clarke, FACS, Xamax Consultancy Pty Ltd, ANU and UNSW
- Mr. Rick Harvey, FACS, FIEAust, CPEng, BE(hons), CTO Lockbox Pty Ltd
- Mr. George Koulakis, Principal Consultant XIPNOS Pty Ltd, ACS Branch Chair (NT) MACS CP.
- Dr. Anthony Overmars FACS CP Director at MOIP Pty Ltd
- Mrs. Jo Stewart-Rattray MEdStud(Psych), CISA, CISM, CRISC, CGEIT, MACS CP, Director of Information Security, RSM Bird Cameron, International Vice President, ISACA
- Mr. Adam Redman MACS, ACS Manager Government Relations and Policy.
- Mr. Rimas Skeivys, MACS (Snr) CP, member of the ACS Victorian Branch Executive Committee, Principle Ugovern.
- Professor Craig Valli MACS CP Dip.Teach(WACAE), B.Ed (ECU), M.Manag.Inf.Sys(ECU), DIT(ECU)
- Professor Vijay Varadharajan, FACS, FBCS, FIEE, FIEAust, FIMA, Microsoft Chair Professor in Innovation in Computing, Director Information and Networked Systems Security Research, Macquarie University, Australia
- Professor Matthew Warren MACS (Snr) BA(Hons), PhD, School of Information Systems, Deakin University.
- Professor Anthony Watson FACS, DV-C(International)and Executive Dean, Faculty Computing, Health and Science Edith Cowan University, Chairman, ACS Security Centre of Expertise
- Tom Worthington, FACS CP, Member of the ACS Telecommunications Board and Adjunct Senior Lecturer, Research School of Computer Science, the Australian National University
- Mr. James Wowchuk, MACS CP and member of ACS NSW Executive.

ENDNOTES

[1] For example, the Council of Europe Convention on Cybercrime celebrates its 10th birthday this year.

[2] http://archive.cra.org/reports/trustworthy.computing.pdf - this conference was attended by ACS Taskforce member Professor Emeritus William J (Bill) Caelli

[3] Over 550,000 Australians are employed in ICT:
http://acs.org.au/index.cfm?action=show&conID=201011180903478965
[4] http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf

[5] For example, commercial-in-confidence, government working papers, data necessary for the control of infrastructure of all kinds - SCADA, and personal data

[6] For example, the US National Initiative for Cybersecurity Education Strategic Plan (August 2011) contains some 50 measurable short-term policy objectives.

[7] http://www.nbn.gov.au/the-vision/digitaleconomystrategy/

[8] http://www.safetyrisk.com.au/2010/05/03/new-risk-management-standard-asnzs-iso-31000/

[9] http://en.wikipedia.org/wiki/Wikipedia:General_disclaimer

[10] http://news.techworld.com/security/7254/wikipedia-hijacked-by-malware/

[11] Page 6: http://www.acs.org.au/attachments/ACSNBNsubmission.pdf

[12] http://www.sfia.org.uk/

[13]
http://www.innovation.gov.au/Industry/InformationandCommunicationsTechnologies/ITIIC/Pages/default.aspx

[14] http://www.acs.org.au/index.cfm?action=list&sgrID=statcomp

[15] http://www-03.ibm.com/security/trusted-identity.html

[16] As the World Trade Organisation notes

> *Technical regulations and standards are important, but they vary from country to country. Having too many different standards makes life difficult for producers and exporters. If the standards are set arbitrarily, they could be used as an excuse for protectionism. Standards can become obstacles to trade. But they are also necessary for a range of reasons, from environmental protection, safety, national security to consumer information. And they can help trade. Therefore the same basic question arises again: how to ensure that standards are genuinely useful, and not arbitrary or an excuse for protectionism.*

[17] http://www.unodc.org/documents/eastasiaandpacific//2011/09/cybercrime-workshop/Meeting_Outcomes_230911_FINAL.pdf

[18] http://cyberwhitepaper.govspace.gov.au/tag/digital-citizenship/

[19] For example: http://www.royalcommission.vic.gov.au/Commission-Reports/Final-Report/Summary/Interactive-Version

[20] Page 59: http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf

[21] http://www.acs.org.au/attachments/cybercrimesubmission.pdf

[22] For example: AUSTRAC, ACMA, ASIC, ACCC, The Australian Crime Commission, The Australian High Tech Crime Centre, APRA, The Office of Film and Literature Classification, The Australian Privacy Commissioner, AUSCERT, Department of Defence, Defence Signals Directorate, Cyber Security Operations Centre, NSW Crime Commission - Computer Crime Team, Victoria Police e-Crime Squad, South Australian Police - Electronic Crime Section, Commonwealth and sector related ombudsman's and consumer affairs agencies.

[23] http://news.dot-nxt.com/2011/10/27/india-proposes-government-control-internet

[24] Some high profile examples including Sony, Vodafone, Telstra and Google have been summarised by the Office of the Information Commissioner : http://www.oaic.gov.au/news/speeches/speech_080911-tp-calma.html

[25]

> *[…] the ALRC proposed that the Privacy Act be amended to include a new Part on data breach notification. The trigger for the requirement proposed by the ALRC was where 'specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual'. Exceptions were provided, for example, where: the specified information was encrypted adequately; it was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the model Unified Privacy Principles (UPPs); or the Commissioner does not consider that notification would be in the public interest. Civil penalties were proposed for failure to notify the Commissioner of a data breach as required by the Act.*
>
> http://www.alrc.gov.au/publications/51.%20Data%20Breach%20Notification/discussion-paper-proposal

[26] Choo KKR 2011. The cyber threat landscape: Challenges and future research directions. *Computers & Security 30 (8): 719-731*

[27] Examples include the Action Fraud website where individual consumers and businesses can report fraud and scams to UK's National Fraud Authority 24/7 (See http://www.actionfraud. org.uk/) and US's Internet Crime Complaint Center (See http://www.ic3.gov/default.aspx).

[28] The Information Systems Audit and Control Association (ISACA) has written extensively on this topic and ACS Taskforce member Mrs. Jo Stewart-Rattray co-authored a publication for ISACA:

> *No security policies, standards, guidelines or procedures can foresee all of the circumstances in which they are to be interpreted. Therefore, if stakeholders are not grounded in a culture of security, there is potential for improper actions.*
>
> *Security should not be considered adverse to mission achievement; where that is so, there is clear evidence that security is a weak part of the overall culture of the enterprise and allows security to be seen as prohibition rather than enablement. Among the rationales for a culture of security is the alignment of security with the enterprise as a whole.*
>
> *The culture determines what an enterprise actually does about security (or any other objective) and not what it says that it intends to do. An effective security culture supports the protection of information while also supporting the broader aims of the enterprise. To sustain a security culture, it is critical to understand whether it was created in a purposeful manner or by "accident."*

A culture of security is not an end in itself, but a pathway to achieve and maintain other objectives, such as proper use of information. The greatest benefit of a culture of security is the effect it has on other dynamic interconnections within an enterprise. It leads to greater internal and external trust, consistency of results, easier compliance with laws and regulations and greater value in the enterprise as whole.

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Creating-a-Culture-of-Security.aspx

[29] http://www.mcafee.com/us/resources/white-papers/wp-reality-of-stealth-crimeware.pdf for a qualified view of the McAfee paper see http://www.zdnet.com.au/cybercrime-2016-a-view-of-the-future-339324825.htm

[30] http://acce.edu.au/nationalcurriculum

[31] http://www.curriculum.edu.au/verve/_resources/National_Declaration_on_the_Educational_Goals_for_Young_Australians.pdf

[32] See also National Initiative for Cybersecurity Education Strategic Plan

[33] http://ec.europa.eu/eqf/terms_en.htm

[34]UNESCO Institute for Statistics, Science & Technology Report (http://stats.uis.unesco.org/unesco/ReportFolders/ReportFolders.aspx?IF_ActivePath=P,54&IF_Language=eng as at 9 Sept. 2011

[35] OECD Main Science and Technology Indicators (eISSN: 2074-4226) as at 9 Sept. 2011.

[36] http://www.science.org.au/events/lectures-and-speeches/documents/npc2011.pdf

[37] A quick survey of Australian ICT R&D would include CSIRO ICT research, DSTO research - which understandably tends to be classified - as well as research conducted by Australian Universities in theoretical and applied ICT research and development of cyber security capabilities and/or the incubation of cyber security companies with good examples in QUT's Information Security Institute, UniSA Information Assurance Group & Forensic Computing Lab, and the Macquarie Centre for Advanced Computing -Algorithms and Cryptography.