COMMUNICATIONS
ALLIANCE LTD

Communications Alliance Submission

to the

Department of Home Affairs Discussion Paper **Australia's 2020 Cyber Security Strategy**

1 November 2019

Page intentionally left blank.

1. Introduction

Communications Alliance* welcomes the opportunity to provide a submission to the Department of Home Affairs Discussion Paper *Australia's 2020 Cyber Security Strategy*.

In our submission, we do not seek to respond to all questions posed in the Discussion Paper but rather offer some general observations that will go to many of the points raised in the Paper.

It is hard to overestimate the importance of a well-executed cyber security strategy: most aspects of modern life are already digitised and 'cyber', and we can reasonably expect that pretty much *all* areas of our lives will be part of the cyber space in the next 10 years.

Therefore, we believe the Discussion Paper is timely and indeed necessary to ensure that the approach to cyber security, including to legislation and regulation in this area, is coherent, proportionate, informed and consultative.

A cyber security strategy is equally an important tool to foster a whole-of-society and economy-wide approach to cyber security and it ought to form the cornerstone to identify, and subsequently remedy, educational, skills and awareness gaps in this area that may exist today.

We commend Government for the wide and public consultation on this important topic and believe that an open-minded, unbiased discussion of this matter will assist with the development of a strategy that is effective, efficient and proportionate while being sufficiently flexible to accommodate for the dynamic environment it operates in.

About Communications Alliance

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

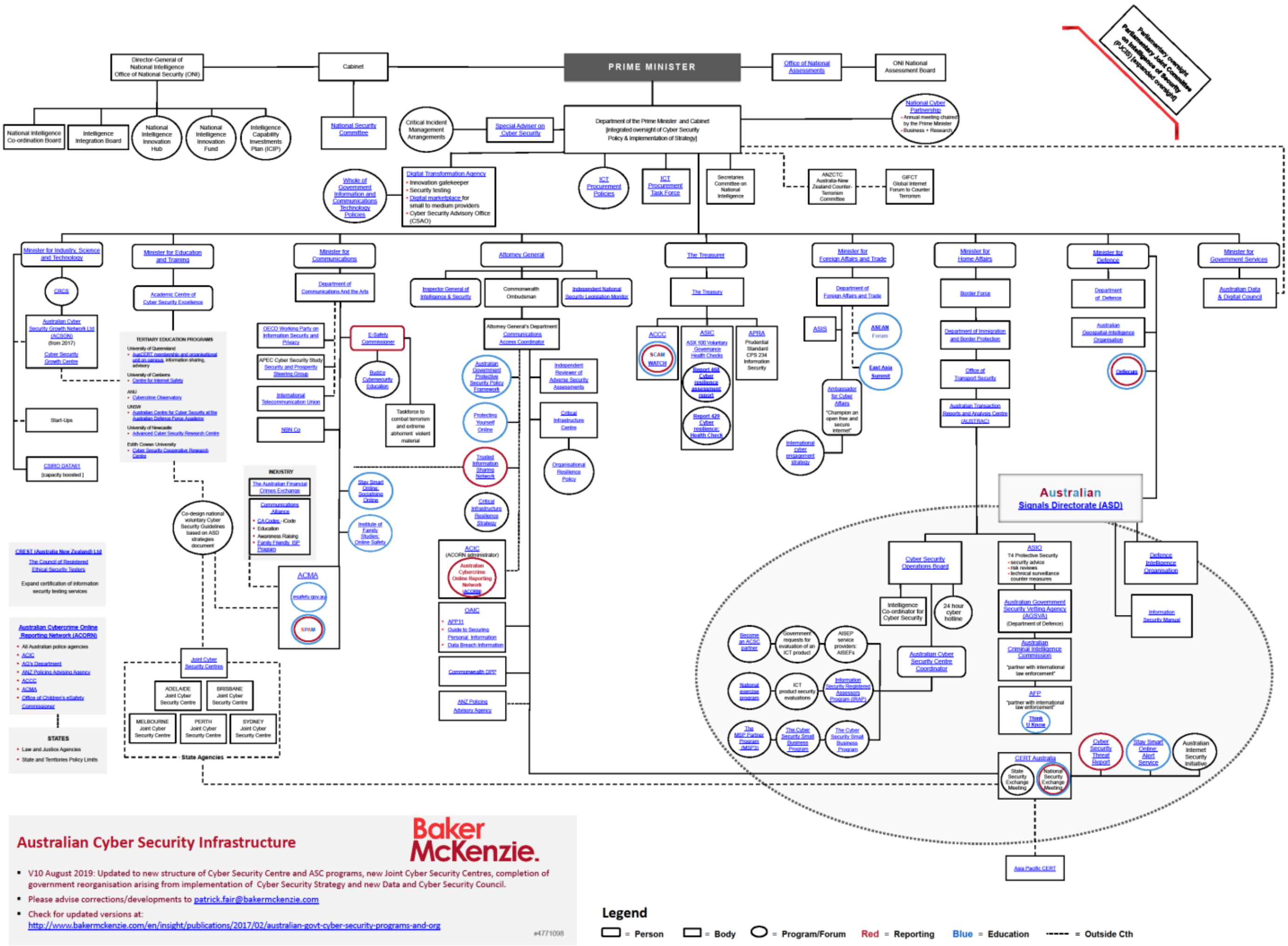
NOTE: *nbn™ is a member of Communications Alliance but has not been involved in the preparation of this submission.

2. Australia's Cyber Security Landscape

A Complex Landscape

As a matter of principle, Government's strategy on cyber security ought to focus on coordination, optimisation and efficiency in the use of Government resources to fight cyber crime and to protect critical infrastructure from unauthorised access and interference.

Unfortunately, the Australian cyber security landscape is characterised by an almost bewildering matrix of Government departments and agencies with an interest in, or portfolio responsibilities, relating to cyber security. These departments/agencies cover a large array of security-related issues and address a multitude of different stakeholders, e.g. telecommunications network operators, businesses across all sectors, the general public, etc. The below diagram illustrates this point. In fact, the landscape is so complex that it is difficult to depict it in a legible format in this submission. For an (expandable) online version of the diagram, see here. (Please note that since drafting this diagram, further changes have occurred which are not yet included, e.g. the Communication Access Co-ordinator and the Critical Infrastructure Centre now sit under the Department of Home Affairs, and ACORN has been replaced by new reporting processes at the Australian Cyber Security Centre etc.)


PRIME MINISTER
Cabinet
Director-General of National Intelligence Office of National Security (ONI)
National Intelligence Co-ordination Board
Intelligence Integration Board
National Intelligence Innovation Hub
National Intelligence Innovation Fund
Intelligence Capability Investments Plan (ICIP)
National Security Committee
Critical Incident Management Arrangements
Special Adviser on Cyber Security
Department of the Prime Minister and Cabinet [integrated oversight of Cyber Security Policy & Implementation of Strategy]
Office of National Assessments
ONI National Assessment Board
National Cyber Partnership
• Annual meeting chaired by the Prime Minister
• Business + Research
Parliamentary oversight Parliamentary Joint Committee on Intelligence of Security (PJCIS) [expanded oversight]
Whole of Government Information and Communications Technology Policies
Digital Transformation Agency
• Innovation gatekeeper
• Security testing
• Digital marketplace for small to medium providers
• Cyber Security Advisory Office (CSAO)
ICT Procurement Policies
ICT Procurement Task Force
Secretaries Committee on National Intelligence
ANZCTC Australia-New Zealand Counter-Terrorism Committee
GIFCT Global Internet Forum to Counter Terrorism
Minister for Industry, Science and Technology
CRCS
Australian Cyber Security Growth Network Ltd (ACSGN) (from 2017)
Cyber Security Growth Centre
Start-Ups
CSIRO DATA61 [capacity boosted]
Minister for Education and Training
Academic Centre of Cyber Security Excellence
TERTIARY EDUCATION PROGRAMS
University of Queensland
• AusCERT membership and organisational unit on campus, information sharing, advisory
University of Canberra
• Centre for Internet Safety
ANU
• Cybercrime Observatory
UNSW
• Australian Centre for Cyber Security at the Australian Defence Force Academy
University of Newcastle
• Advanced Cyber Security Research Centre
Edith Cowan University
• Cyber Security Cooperative Research Centre
Minister for Communications
Department of Communications And the Arts
OECD Working Party on Information Security and Privacy
APEC Cyber Security Study Security and Prosperity Steering Group
International Telecommunication Union
NBN Co
E-Safety Commissioner
Budde Cybersecurity Education
Taskforce to combat terrorism and extreme abhorrent violent material
INDUSTRY
The Australian Financial Crimes Exchange
Communications Alliance
• CA Codes - iCode
• Education
• Awareness Raising
• Family Friendly ISP Program
Stay Smart Online: Socialising Online
Institute of Family Studies: Online Safety
Co-design national voluntary Cyber Security Guidelines based on ASD strategies document
ACMA
esafety.gov.au
SPAM
CREST (Australia New Zealand) Ltd
The Council of Registered Ethical Security Testers
Expand certification of information security testing services
Australian Cybercrime Online Reporting Network (ACORN)
• All Australian police agencies
• ACIC
• AG's Department
• ANZ Policing Advising Agency
• ACCC
• ACMA
• Office of Children's eSafety Commissioner
STATES
• Law and Justice Agencies
• State and Territories Policy Limits
Joint Cyber Security Centres
ADELAIDE Joint Cyber Security Centre
BRISBANE Joint Cyber Security Centre
MELBOURNE Joint Cyber Security Centre
PERTH Joint Cyber Security Centre
SYDNEY Joint Cyber Security Centre
State Agencies
Attorney General
Inspector General of Intelligence & Security
Commonwealth Ombudsman
Independent National Security Legislation Monitor
Attorney General's Department Communications Access Coordinator
Australian Government Protective Security Policy Framework
Protecting Yourself Online
Trusted Information Sharing Network
Critical Infrastructure Resilience Strategy
Independent Reviewer of Adverse Security Assessments
Critical Infrastructure Centre
Organisational Resilience Policy
ACIC (ACORN administrator)
Australian Cybercrime Online Reporting Network (ACORN)
OAIC
• APP11
• Guide to Securing Personal Information
• Data Breach Information
Commonwealth DPP
ANZ Policing Advisory Agency
The Treasurer
The Treasury
ACCC
SCAM WATCH
ASIC
ASX 100 Voluntary Governance Health Checks
Report 468 Cyber resilience assessment report
Report 429 Cyber resilience: Health Check
APRA
Prudential Standard CPS 234 Information Security
Minister for Foreign Affairs and Trade
Department of Foreign Affairs and Trade
ASIS
ASEAN Forum
East Asia Summit
Ambassador for Cyber Affairs
"Champion an open free and secure internet"
International cyber engagement strategy
Minister for Home Affairs
Border Force
Department of Immigration and Border Protection
Office of Transport Security
Australian Transaction Reports and Analysis Centre (AUSTRAC)
Minister for Defence
Department of Defence
Australian Geospatial-Intelligence Organisation
OnSecure
Minister for Government Services
Australian Data & Digital Council
Australian Signals Directorate (ASD)
Cyber Security Operations Board
Intelligence Co-ordinator for Cyber Security
24 hour cyber hotline
Australian Cyber Security Centre Coordinator
Become an ACSC partner
Government requests for evaluation of an ICT product
AISEP service providers: AISEFs
National exercise program
ICT product security evaluations
Information Security Registered Assessors Program (IRAP)
The MSP Partner Program (MSP3)
The Cyber Security Small Business Program
The Cyber Security Small Business Program
ASIO
T4 Protective Security
• security advice
• risk reviews
• technical surveillance counter measures
Australian Government Security Vetting Agency (AGSVA) (Department of Defence)
Australian Criminal Intelligence Commission
"partner with international law enforcement"
AFP
"partner with international law enforcement"
Think U Know
Defence Intelligence Organisation
Information Security Manual
CERT Australia
State Security Exchange Meeting
National Security Exchange Meeting
Cyber Security Threat Report
Stay Smart Online Alert Service
Australian Internet Security Initiative
Asia Pacific CERT
Legend
▭ = Person
▭ = Body
○ = Program/Forum
Red = Reporting
Blue = Education
---- = Outside Cth

Australian Cyber Security Infrastructure

Baker McKenzie.

- V10 August 2019: Updated to new structure of Cyber Security Centre and ASC programs, new Joint Cyber Security Centres, completion of government reorganisation arising from implementation of Cyber Security Strategy and new Data and Cyber Security Council.
- Please advise corrections/developments to patrick.fair@bakermckenzie.com
- Check for updated versions at: http://www.bakermckenzie.com/en/insight/publications/2017/02/australian-govt-cyber-security-programs-and-org

#4771098

Source: Baker McKenzie

As noted in previous submissions on this issue, prior to the development of a national cyber security strategy, it would be important to gain a better understanding of the precise roles and responsibilities of each of the involved departments/agencies, and where their responsibilities intersect and overlap. It appears that a better coordination of the current spread of agencies and programs and more focussed spending on a single national point of access would be likely to result in a more effective approach to cyber security. It would also serve to address what must be an enormous and, at times, inefficient coordination burden on the involved departments and agencies. This is not to say that all cyber-related functions ought to come under a 'single roof' as it will be important to retain appropriate checks and balances in a potential consolidation process. However, it seems that a streamlining of organisations, functions and processes would be useful.

We note that initial steps have been taken in this direction with the establishment of the Australian Signals Directorate (ASD) as a statutory agency and the collocation of the Australian Government's cyber security functions in ASD's Australian Cyber Security Centre (ACSC). However, we note with concern that Appendix A (Progress against Australia's 2016 Cyber Security Strategy) to the Discussion Paper lists Action 3, Streamline the Government's cyber security governance and structures, as 'complete'. In our view, more ought to be done in this respect and the streamlining process cannot be considered complete.

Apart from potential efficiency gains, we also note that until such an approach is defined, there remains the question as to who would be the arbiter of security risk within the current landscape. We believe that there ought to be a unified directory (or 'single point of truth') of information regarding cyber threats and responses where relevant professionals and members of the public can receive further targeted awareness information (and alerts depending on criticality).

It should also be noted that the chart above lists only cyber security-related organisations and initiatives and some online safety related activities, and does not include any other cyber-related Government organisations. While we do not have access to a similar chart regarding the overall cyber-related activities by Government agencies, it seems likely that a similarly complex picture exists.

It is important to ask which other areas of responsibility in the field of cyber engagement (other than cyber security) Government, industry, academia and other stakeholders ought to address to fully harness the advantages of the cyber space to Australia's (and global) advantage. For example, the international harmonisation of data and privacy laws, the development/adoption of open technology standards, the identification of a toolbox of appropriate and effective risk management measures and a coherent (and timely) approach to the proliferation of the internet of things (IoT), artificial intelligence (AI), cloud platforms, 5G and fibre networks immediately come to mind in this context.

It also seems difficult – as already evident in practice – to delineate cyber security from data privacy, national security and online safety (eSafety).

International Context

It is hard to contemplate an efficient and effective national cyber security strategy in isolation, i.e. outside an international context and international cyber security engagement strategy.

The cross-border nature of data, computer systems, networks and increasing globalisation necessarily make any viable cyber strategy an international affair, especially for open economies that rely on international trade and relationships for the running of their economies and their national security.

Naturally, as owners and operators of the underlying infrastructures that enable much of the cyber world, the communications and IT industries have a strong interest in the development of an effective and coherent international cyber security engagement strategy. However, we note that the digitisation of all aspects of the modern state mean that all industries and sectors as well as citizens ought to be part of this important discussion.

It appears that the Discussion Paper does not place Australia's strategy sufficiently into such an international context. Further consideration ought to be given how the strategic approach envisaged for Australia relates to efforts in other nations, especially Australia's key trading partners and global industry standardisation organisations (e.g. 3GPP) and alliances (e.g. GSMA), and how it would contribute to the unification of global standards, harmonisation of privacy laws, appropriate and effective risk management measures and international cooperation.

It is also likely that the complex cyber security landscape discussed above not only makes the pursuit of a unified and effective cyber security strategy on a national level difficult, but equally impedes the execution of an effective and efficient engagement on an international level.

Policy Context

Looking at a wider policy context, it appears that the creation of a legislative framework for cyber security, national security and online safety precedes the development of the cyber security strategy itself, i.e. the logical chronological order of actions has been reversed, with elements (pieces of legislation) of a larger strategy being considered before the strategy itself (Australia's 2020 Cyber Security Strategy) has even been defined.

For example, the Telecommunications Security Sector Reform (TSSR) was developed throughout the years 2014 to 2017 and came into force in September 2018. Similarly, in December 2018, Australia saw the passage of the (highly controversial) *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018,* with potentially far-reaching consequences for the cyber security of Australian networks, businesses and the public at large. It has been noted in public debate that this legislation may make it more difficult for Australian-based organisations to compete with overseas rivals who are not subject to similar legislation. And in March 2019, with a view to not providing a platform for abhorrent violent material and to protecting Australian's from such content, the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* became law within two days of being introduced into Parliament. None of these pieces of legislation appear to have formed part of the 2016 Cyber Security Strategy. The Discussion Paper also does not take account of the challenges that the sometimes ad-hoc and piecemeal approach to making legislation poses for Australian industry and society at large.

As noted above, while not all of the above pieces of legislation directly aim at cyber security, given the blurring lines of cyber security, national security and online safety, it would be desirable to either clearly delineate cyber security from the other two (which may be very difficult as highlighted by the debate around the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*), or to look at the three issues in a wider context and with a 'big picture' lens.

As we will outline below and as touched upon in the Discussion Paper, Australia needs to engage in a broader debate about the roles and responsibilities of Government, industry, end users and other stakeholders in a world where (almost) every aspect of our lives will be digitised and enabled by communications technology, data analytics, artificial intelligence etc.

3. Digital Technologies as an Enabler of our Lives

Already today, large parts of our everyday lives are only possible due to the omnipresence of pervasive, underlying digital technologies. Soon, our world will be almost exclusively digital. Many of these technologies are enabled by our industry's communications infrastructures such as physical networks, cloud systems and storage, and digital platforms. Indeed, it has become increasingly difficult to delineate between carriage services provided over provider infrastructure in a classical sense and services that are running 'over the top' of carrier networks, such as messaging, content and location services. So far, regulation and legislation has taken a technology-based approach with responsibilities mostly being imposed at an infrastructure layer. However, it has become clear that any robust legislative framework and cyber security strategy will need to take a technology and platform neutral approach in order to adequately address today's cyber security challenges. However, no matter where such a line is being drawn – if it is necessary to draw such a line at all – it is clear that the security control zone and allocation of responsibilities for the use – and mis/abuse – of these systems and infrastructures is complex.

Our industry cooperates with Government agencies in many areas to attempt to minimise cyber incidents, crimes committed through the use of the cyber space and to combat the harmful effects that may arise through material accessible on the internet. As indicated in the Discussion Paper, carriage service providers also comply with obligations, amongst others, to do their best to make their networks resilient from unauthorised access and interference and to maintain competent supervision and control of their networks and systems.

Unfortunately, our industry observes a tendency, as a default position, to shift responsibility – and the associated costs – for addressing cyber harms to the providers of such infrastructure. While it is clear that the ICT industry has an important role to play, we believe Australia needs a broad and balanced discussion on the principles and responsibilities for cyber security that ought to apply in an all-digital world. This discussion will also need to include the relationship of cyber/national security and privacy rights and civil liberties more generally.

It is very tempting to delegate responsibility for cyber security, national security and/or online safety to industry players which may technically, to varying degrees, be able to address some (but certainly not all) of the cyber harms. Naturally and in part due to the long timeframes involved, it appears less appealing to invest the very large amount of resource that would be required to educate all layers of society and the economy about their individual responsibilities in relation to cyber security and, importantly, to impart the required knowledge to be able to take on such responsibilities.

Cyber security involves many elements and stakeholders. An all-industry, full-society approach to collaboration is essential to enhancing systematic cyber security governance.

4. Cooperation and Information Sharing

As the Discussion Paper notes “it is becoming increasingly important for [Government action against cyber threats] to be supported through partnerships and collaboration with industry.”[1] We agree that close two-way cooperation and sharing of threat information between Government agencies and industry players will be critical to a successful approach to cyber security.

However, our industry finds that the partnerships envisaged in theory have not always translated into effective collaboration in practice. Our members’ experience with the implementation of the TSSR may serve as an example:

The Explanatory Memorandum to the TSSR Act expresses a legislative intent for a collaborative, bilateral sharing process around the notification regime that the TSSR introduces. Such sharing of information would allow carriers, where appropriate, to alter the way they design, protect and manage their networks.

Unfortunately, carriers feel that this bilateral sharing of threat information has not eventuated. Twelve months after the legislation came into force, carriers report that they have still not been briefed on the specific weaknesses in their networks or specific threats to the communications sector – if such exist – that agencies would consider elevating the risk for cyber and national security. This lack of sharing of existing threat information cause practical issues as carriers find it more difficult and/or costly to protect their networks and facilities, as required by the law. Existing forums, such as the ASIO Business and Government Liaison Unit (BGLU) and the Trusted Information Sharing Network (TISN), while being referenced in the TSSR material provided by the Critical Infrastructure Centre, have not enhanced their role of information sharing specific to the telecommunications sector.

Some carriers also report that agencies are not forthcoming with information as to benchmarks or criteria against which potential changes to their networks, which are notifiable in many instances, would be assessed. Similarly, some carriers say they find it difficult to informally engage with the relevant authorities, who are often reluctant to provide meaningful information in response to informal requests.

[1] p.15, *Australia’s 2020 Cyber Security Strategy – A call for views*, Department of Home Affairs

Some carriers also indicate that they feel the burden of proof is, at times, reversed, i.e. it appears that they are being asked to 'prove' that an intended change to their networks or systems does not compromise their ability to comply with the security obligations, rather than being presented with evidence that these changes would compromise their ability to comply.

The Discussion Paper appears to follow similar thinking and highlights what industry sees as an imbalanced approach to sharing/reporting. The paper notes the lack of a requirement on businesses to report significant cyber incidences, thereby leaving Government potentially unaware of incidents that threaten Australia's security.[2] However, the paper fails to equally contemplate the need for obligations on Government to share information with industry, particularly with businesses that provide critical infrastructure.

The Discussion Paper raises the question whether Government should be able "to proactively identify any vulnerable systems to address Australia's exposure and better assist the community."[3] The paper appears to suggest that Government potentially ought to be given the power to access and mange critical infrastructure and systems – more so than already possible under the new powers of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. If this is indeed contemplated, industry will oppose it vehemently. Instead, as discussed above, Government ought to be encouraged to share threat information with industry in a timely fashion to ensure that a true two-way sharing relationship emerges. However, the management of networks and systems must solely remain with the owners or operators of such infrastructure, who are best placed to mitigate against threats and to minimise the risks of unintended consequences.

Collaboration among relevant stakeholders can encompass a number of practical areas, including information exchange, threat analysis, performance analysis, testing, sharing of best practices and encouraging cutting-edge research. Given the proliferation of the IoT, cooperation with other connected infrastructures such as energy, transport, health care, resources, automated manufacturing etc. will be of increasing importance.

Within the telecommunications sector, industry would prefer a single framework of protected sharing to the existing mandatory data breach notification approach. Government ought to consider creating a legal framework of the kind proposed in the *US Cyber Intelligence Sharing and Protection Act*. This legislation creates protection and immunities for the sharing in good faith of cyber intelligence and would be an advance to the informal arrangements in place for the Trusted Information Sharing Network (TISN) which do not allow for a sufficiently timely exchange of information.

Information sharing of this nature is overdue and is necessary to ensure consistent high-level protection of critical infrastructure. However, under any approach (legislated or informal) the benefits, communication channels and scope (terms of reference) of information sharing must be clear to all stakeholders to ensure their ongoing engagement and commitment to established processes.

Regular working groups and fora to bring industry and Government together to discuss cyber security issues would assist, especially if Government can offer expertise or advice to business on the current threats and work together – building on the work of the Joint Cyber Security Centres (JCSCs) – to identify future areas of focus. Information about security breaches suffered by Government agencies and information related to espionage related cyber attacks should be shared by Government with relevant industry stakeholders, subject to protected sharing.

International Cooperation

We identified a number of regional and global fora that engage with cyber security and that, we believe, are relevant to Australia's strategic interests. However, it is not always clear

[2] p.8, *Australia's 2020 Cyber Security Strategy – A call for views*, Department of Home Affairs

[3] p.10, Case Study, *Australia's 2020 Cyber Security Strategy – A call for views*, Department of Home Affairs

to us whether Australia engages in all of those fora, and if so, through which organisation/means of representation it participates, whether this engagement is effective and whether additional or different efforts would be required, particularly also in areas that do not specifically relate to security.

We would also like to see a comprehensive and structured consultation process to assist preparing positions that are put forward at regional or global fora. We are not aware of such a structured approach but note that industry does receive occasional ad-hoc requests for input.

Global fora:

- Organisation for Economic Co-operation and Development's (OECD) Working Party on Security and Privacy in the Digital Economy
- Internet Governance Forum
- United Nations (UN) Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
- International Telecommunication Union
- Global Forum on Cyber Expertise
- Global Conference on Cyberspace
- Commonwealth Telecommunications Organisation

Regional Fora

- Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group
- Association of Southeast Asian Nations (ASEAN) Cyber security Cooperation Strategy
- East Asia Summit

Australian businesses, as most other nations, make use of commercial advantages outside Australia and outsource some of the strategic and/or operational functions to other countries, e.g. European Union, India, Philippines, US, UK, Singapore and Japan. China plays an important role independent of any potential outsourcing arrangements due to the large quantity of devices that originate from there and the potential to greatly impact any nation's cyber space. An analysis of businesses' data sharing arrangements as set out in privacy policies may reveal further countries of interest in this context.

5. Education

Cyber Security Specialist Resources

One of the biggest challenges posed by cyber security for many organisations, and Australia in general, is the constant need for expert resources to cope with the evolving scope of cyber security threats. This demand for cyber security specialists is not met with an equal supply available to all Australian businesses. The shortage of supply may be partly a result of lacking tertiary (and other) education opportunities in this field and is likely to be exacerbated by fierce competition for qualified resources from other well-resourced sectors, such as the financial services and insurance sectors. As matters stand today, telecommunications industry members have highlighted a shortage of supply of specialist resources in various areas, e.g. in forensics, penetration testing, incident management and risk assessment.

In addition, it would be prudent to broaden the scope of any strategy to address skill shortages to also include the production of experts in policy, psychology, law etc. which are all areas that will play an important role in long term strategies to enhance cyber security.

Against this background, industry urges Government to develop a cyber security strategy that includes a targeted program to develop and retain Australia's expertise in this area to ensure that local resources are available to all industries and all players within those industries. When developing such a program, it will be key to ensure that an end-to-end coverage of the cyber security chain will be achieved. In this context, it could be useful to investigate international models for developing cyber security capacity, their effectiveness and, where feasible, applicability in an Australian context.

Given the fast pace of evolution in the cyber security arena combined with the level of technical expertise required for practical industry application, educational institutions/academia and industry from all sectors must cooperate very closely to ensure that education remains relevant and meets demand as technology evolves. Consequently, any education program ought to include mentoring initiatives, graduate programs (including substantial work experience), and grant schemes aimed at fostering innovation and creativity in this space.

Cyber Security Literacy of Individuals and Businesses.

As social engineering is a key element of cyber crime, it is essential that individuals and particularly small businesses are being educated on the basics of IT security. A concerted coordinated effort is required to achieve high levels of awareness, education and implementation of security measures. We contend that the diverse array of education and awareness initiatives across federal and state agencies is not conducive to achieving this aim. It is recommended that a strategy be developed that analyses the key targets of educational initiatives, focuses the messaging and activities of each program accordingly and ensures a coordinated delivery.

With the accelerating proliferation of the IoT, distributed cloud platforms, and artificial intelligence, the challenge of good cyber awareness, literacy and ultimately security equally moves from being a must for businesses to being imperative for all individuals in Australia who will own or operate an ever-increasing number and variety of smart devices, computers, consumer electronics, etc. A coordinated Government-led education campaign is required to push and actively promote the safe(er) use of social media, email and the internet. Currently, Government initiatives like SCAM and the Stay Smart Online Alert Service go in this direction, but require individuals to actively search for information and subscribe, rather than pushing information out to the general public. There is a role for Government to foster an instinctive understanding by the general public that cyber security is part of daily life and routine – just as much as road safety, environmental consciousness and healthy lifestyles ought to be. Such efforts must include a far greater awareness that stronger password protections for any device connected to the internet is required to protect individuals' privacy from intended or accidental intrusion. Campaigns for improved sun protection (e.g. SunSmart, Slip, Slop, Slap) or campaigns targeting nicotine addiction may be instructive as to how to bring cyber security at the forefront of citizens' minds and to adopt healthy cyber attitudes.

While larger Australian businesses are likely to have access to more financial resources to provide attractive employment packages for cyber security professionals, smaller businesses may not be able to compete with cyber security experts' expectations of remuneration. Importantly, smaller businesses may not understand the need for investment in this area in the first place as they may fail to adequately perceive the risk posed by cyber crime.

In any case (for small and large businesses alike), resourcing for the risk of cyber crime always competes with resourcing for other business priorities that are being perceived of delivering more certain and tangible benefits to the company, e.g. the evolution of existing products, innovation of new products, network expansion (in a telecommunications environment) and the general commercial requirement to satisfy customer needs.

It may be worth considering whether programs similar to CitySwitch[4], which includes the use of awards and certification levels, might be used to encourage (particularly small and medium sized) businesses to implement better cyber security measures.

Opportunities

While cyber security poses challenges for Australia, we can see opportunities for Australia to become best-in-class and a world leader in identifying and managing cyber security threats and education campaigns. However, as indicated above such opportunities will only arise on the back of a single cohesive, collaborative nation-wide approach to cyber security that is embraced by Government, industry and the public. Given the fragmented and at times uncoordinated and piecemeal approach to cyber security, we fear that Australia is not positioning itself to fulfil aspirations of best-practice and becoming an exporter of cyber security related goods and services. Quite to the contrary, it currently appears that Australia is losing qualified professionals to overseas locations without necessarily repatriating the expertise that those individuals have gained abroad.

Industry's view (and that of international experts) is that the passage of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* is an effective 'smack in the face' for any ambitions to promote Australia's cyber security industry. This issue is not the result of a global misunderstanding of the workings of the Act. Rather, the damage being done to Australian industry is due to technology buyers and investors around the world having listened to the strong body of international and Australian expert opinion and business advice on the risks that the Act creates for the security of Australian-manufactured technology equipment and systems.

Consequently, we again urge Government to amend the Act to limit the damage to Australian exporters of cyber security products and services. Communications Alliance has provided submissions detailing proposed amendments, to both the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and to the Independent National Security Legislation Monitor (INSLM).

6. End-User Trust

It will be difficult or even impossible to address the issue of end-user trust in Australia's cyber security without also dealing with the question of how to balance civil liberties with the (actual or perceived) need by Government and industry to interfere with those civil liberties to safeguard against cyber (or other) harms.

While others will be better placed to lead the debate on this matter, we do highlight that the recent tendency to rush legislation through Parliament without proper consultation with industry and other stakeholders and disregarding expert advice, is detrimental to an informed debate on the consequences of such legislation on this delicate balancing act.

The Discussion Paper raises the question of whether consumers are sufficiently informed about the cyber security of goods and services that they purchase and whether those goods and services are actually secure. This question is even more pertinent in the context of the IoT and the expectation that in 2022 the average household will have 37 connected devices, ranging from smartphones to connected cat flaps, televisions, digital assistants, baby monitors, security cameras and refrigerators. The fact that, in near the future, everything will be connected makes a 'secure by design' approach imperative.

[4] CitySwitch is a program that supports commercial office tenants/building managers to improve office energy efficiency through the provision of a range of services, with the ultimate aim of achieving a 4 star or higher NABERS energy rating. It helps participants to use a structured approach to planning and implementing energy efficiency projects with the aim of saving time and money and helping to build participants' own capacity to embed sustainability within their corporate structure.

While security for traditional mobile devices such as mobile phones, tablets etc. would benefit from further improvements, overall security of such devices and the concept of security by design for those devices is reasonably well-established. However, as security scares around hacked baby monitors and smart TVs demonstrate, security for many devices connected to the internet leaves a lot to be desired.

One way of driving this outcome would be for industry to develop a trust mark for connected consumer devices which, similar to the water efficiency rating of washing machines or the health star rating on packaged food, provides consumers with a simple and clear indication of the security of the connected device that they are intending to use. If consumers are adequately educated about the benefits of secure products (and the significant risks of those that are less secure), they will demand and buy secure products, thereby driving a greater focus on secure design on the part of developers and manufacturers. Over time, it is conceivable that shopping outlets will seek to differentiate themselves from competitors by only selling devices with a certain cyber security star rating, similar to supermarkets advertising that the food they are selling does not contain any artificial colouring.

Significant initial work has been undertaken by our members and members of the IoT Alliance Australia (IoTAA), also a not-for-profit organisation, to develop such a trust mark. It would be timely and appropriate for Government to provide funding to further this worthy initiative.

It should be clear that the development of the criteria and security standards that form the basis of any trust marks must be developed in an international arena, with subsequent rigorous enforcement by the responsible national agencies.

7. Regulatory Frameworks

Self-Regulatory Frameworks

Industry believes that the use of a prescriptive legislative framework and rules-based regulation in a fast-moving environment such as cyber security is inappropriate as they lack flexibility and rapid adaptability to accommodate technological change. It is equally important that any framework is outcomes-based rather focused on detail as to how to achieve the desired outcomes.

However, we see a need for industry codes, standards, and best practices. The NIST Guideline and the iCode serve as good examples of industry documents that have been designed for 'real world' application by industry players of varying sizes. Such codes, standards and guidelines are helpful to ensure that all providers have access to a set of minimum standards to implement in their businesses in a way that suits their business models and their business activities, e.g. in a maturity model approach. This is particularly important for key assets that require protection, e.g. the protection of credit card details on the basis of the PCI-DSS standards.

Furthermore, industry supports global efforts towards a standardised security development and solution design, referred to as Security Assurance Methodology (SECAM).[5] There is a real risk that uncoordinated global efforts in this area will lead to a diverging set of security requirements, which would jeopardise not only interoperability, but make security that much more complex to guarantee. Global standards and best practices are therefore fundamental to the efficient handling of threats – especially given that a large share originate across national borders – as well as to building economies of scale, avoiding fragmentation and ensuring interoperability. Therefore, it is essential that stakeholders, including operators, vendors, regulators, policymakers and IT-focused companies as well as

[5] Security Assurance Methodology (SECAM) establishes security requirements not just for products but also for product development processes. According to proposed SECAM rules, accreditors will verify a 3GPP manufacturer's overall capability to produce products that meet a given set of security requirements, which will eliminate the need for explicit certification on a per product basis, while also encouraging a solution based view.

players from other industries, work together to set common and open security standards that specify what needs to be secure and protected, rather than mandate the use of a particular technology, i.e. industry supports an independent process compliance/validation scheme rather than fragmented, national certification schemes for devices and IT systems, or expensive, time consuming certifications like, for example, the Defence Level Common Criteria (CC).

Inter-jurisdictional frameworks:

As all parties involved are likely to attest, inter-jurisdictional investigations of cyber issues can be exceedingly difficult due to lack of sovereignty, lack of resources, diverging or even conflicting priorities or all of the above. Depending on the matter at hand, even national investigations or initiatives can be cumbersome due to different legal requirements and/or Governmental roles and responsibilities.

Companies operating across borders or wanting to outsource parts of their operations or data storage equally feel the burden of having to comply with different legal requirements.

The creation of inter-jurisdictional frameworks will be key to the maximisation of the economic and social benefits and the minimisation of security risks that the cyber space brings with it. Unfortunately, one can also assume that this task will also be one of the most difficult to achieve. Nevertheless, considerable efforts by Government, private sectors and academia ought to be made to progress internationally applicable and enforceable frameworks as quickly as possible.

The cross-border nature of data, its increasing commercial value – in large parts due to vastly improved analytical capabilities (big data analysis) – and the soon complete digitisation of our civil societies, defence systems and Government apparatus, mean that ownership, sharing and protection of data across borders and jurisdictions will be vital for the maximisation of economic benefit and the smooth operation of societies, including the prevention of crime and the enforcement of law. With significant parts of the world's population are still without regular or no access to the internet, a well-designed international cyber engagement strategy would provide a useful blueprint for developing nations without such strategies once they reach a critical point of digitisation. Those developing nations themselves, but also (maybe even more so) highly digitised nations around the globe stand much to gain from a secure and coordinated growth of the cyber space of the developing world.

It is, therefore, imperative that we engage on an international level to drive the development of international data frameworks. For example, it has been suggested to tie the protection of data to the location of users, i.e. to create a 'virtual sovereignty', by binding the laws of each country to the location of the user who created the data at the time the data was created.[6] While this would require international treaties and is not without challenges, e.g. when companies would be forced to abide by laws of states that they do not consider democratic etc., it appears that an international approach to data ownership, sharing and protection is unavoidable. While we do not intend to advocate for a specific approach of how to address this complex issue, the above example may be illustrative of the kind of inter-jurisdictional efforts that are required.

The key issue – and difficulty – to be considered when designing data and privacy frameworks will be how to maximise the economic benefit from data by allowing the private sector and academia to exploit its economic value or to use it for research that directly or indirectly will generate benefits for society while simultaneously allowing Government to protect its citizens.

However, independent of the aforementioned difficulties of creating inter-jurisdictional frameworks, we believe that ultimately a key objective of the international cyber security strategy must be the pursuit of effective (yet balanced) enforcement mechanisms (of inter-

[6] Andrew Burt, "Virtual sovereignty can help govern our data", 6 February 2017, Financial Times

jurisdictional frameworks) at an international level that will result in collective action against the source of cyber threats and will facilitate the development of the cyber space to maximum social and economic benefit.

8. Conclusion

Communications Alliance looks forward to continued engagement with the Department of Home Affairs and other relevant stakeholders on this important topic.

We share Government's desire to create a robust, effective and efficient cyber-security framework that appropriately allocates responsibilities across all actors involved, and that enables all Australians to adequately protect themselves against the risks that come with it while enjoying the enormous benefits that it affords to all of us.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507