Submission for Australia's 2020 Cyber Security Strategy

(A) Introduction

First I would like to congratulate Dept. of Home Affairs and Australian Government for their Call for Views on 2020 Cyber Security Strategy paper which raises several pertinent issues in cyber security for the digital era. I very much welcome this opportunity to provide inputs to the formulation of the next phase of Australia's Cyber Security Strategy.

This enquiry is a timely one, given the dramatic developments in technologies such as Cloud Infrastructures, Internet of Things and Big Data, and their impact on various business sectors and our daily lives. Along with the phenomenal growth in technology and digital economy, there has been a growth in technology related threats and attacks. Hence the need to take further measures to maintain and further improve confidence on the digital infrastructures and services among the different stakeholders such as end users, SMEs as well as corporate and government organizations. In this regard, we believe the government has a critical role to play in developing not only suitable policies and regulations but also facilitating a safe and trusted digital environment. Industry is not a monolith comprising SMEs to large corporations both national and international and of course plays a major part in making products and services that need to be secure and trustworthy. The users form a vital part of this ecosystem who are impacted both by the products industry offer and by the government policies and regulations. Once again users are heterogeneous like the technology they use. This multi-faceted nature of cyber security involving technological, business, legal and social aspects clearly poses many significant challenges. It is pleasing to see several of these challenges reflected in the questions in this Cyber Security Strategy 2020 Call. We will now address these questions in turn and give our comments and suggestions.

(B) Q1: Cyber Threat Environment and Government Focus

It is clear that technological applications have become pervasive. In particular, in our view, the combination of Internet of Things (IoT), cloud and big data applications together with cyber physical systems are and will be dominating the technology space in the many years to come. We believe this dramatically increases the ***cyber security threat velocity*** – with (i) more and more vulnerabilities and attacks arising with different technologies (e.g. due to systems of systems), (ii) an evolving set of bad guys (e.g. from hacker groups, to corporate espionage, to state actors), (iii) attacks happening at zero time (with no grace period) and (iv) attacks becoming sophisticated (due to easily available tools). This is the cyber threat environment we are dealing with. As mentioned above, all the parties involved (governments, industry and users) need to play their parts in containing and mitigating the cyber security threat velocity in such a pervasive technological environment.

We believe at least **three areas where government should focus on** which include:

- ***Safety and protection of critical infrastructures:*** This includes not only infrastructures such as utilities, energy and transport, (which are increasingly undergoing digital transformations), but also digital infrastructures (such as data centres and smart city infrastructures), which are critical for the national economy.
- ***Security and trust on IoT devices*****,** with the proliferation of devices being connected to the Internet leading to amplification of threats and attacks (including in the critical infrastructure space). We have deliberately highlighted the IoT technology due to its ubiquitous connectivity (and use of other powerful capabilities such as cloud) is forcing us to reconsider our definitions of sectors, perimeters, trust, and control.
- ***Security of supply chain****:* As most systems consists of many components/products coming from different manufacturers and providers; furthermore many of these components/products are being manufactured by SMEs which form a lion share of the Australian economy. Despite their often-constrained resources, SMEs are essential stakeholders in any effort to enhance cybersecurity—particularly in light of their role in the supply chain—and their needs must be better addressed. The focus on the supply chain security can help to mitigate one of the root causes of the proliferation of security threats in the digital ecosystem.

(C) Q2-Q3: Responsibility of Managing Cyber Security Risks

The current situation with respect to responsibility of cyber security can be characterized as follows:

- End users: It places a significant amount of responsibility on the end users for managing their own security and hence making them bear a fair amount of the risk and costs associated with it.
- Industry: There are different levels of maturity (w.r.t cyber security) among the providers of goods and services: (i) some have a good understanding of their responsibilities concerning security *and* are serious about meeting their responsibilities, (ii) while some others though aware of the security implications of their products but are not serious about taking their responsibility, (iii) whereas some others are not even aware, and (iv) others are aware but are constrained by resources in their ability to assume their responsibilities.

(a) ***We believe there is a need to shift the responsibility for secure ecosystem more towards industry, transferring the responsibility to providers of goods and services for managing a greater portion of cyber security risks.***

- First, the providers of goods and services have a better understanding of their own products and hence in a better position to take responsibility, compared to the end users (information asymmetry between vendors and their customers about the products).
- As technologies become more and more complicated, this need to shift responsibility increases even more. It is much more than technical vulnerabilities, but also on the overall impact of externalities. If malware causes a business to lose money, in addition to considering loss prevention, but also ensure that the liability falls on the party most capable of mitigating the risk.

E.g. car companies should bear the cost of unsafe software causing accidents. If autonomous vehicles are bundled with insurance, then the incentives may be broadly in the right place, at least for the first purchaser; but still have to consider how used vehicles will get security and safety patches, and the cost of their insurance.

- Furthermore, of course businesses derive benefits (in terms of revenue and profits) and hence they have a clear obligation to take more responsibility concerning security of their own products and services.

(b) *Concerning end users, we believe the need to emphasize certain aspects of their responsibility.*

- For instance, with consumer IoT devices, it is important to educate/encourage/assist (or even enforce that) the consumers to (i) register their consumer products upon purchase, and (ii) change the security settings (e.g. admin passwords on their devices). *This must become an integral part of cyber hygiene* (such as putting seat belts in cars before driving). Initial best practices can include requirements to mandate that IoT devices be rendered unusable until users first change default usernames and passwords. Weak usernames and passwords would be rejected by the device.
- If and only if the manufacturer knows the existence of their product in the digital ecosystem, they can take the responsibility for security of their products; this is a major issue when it comes to IoT devices as device manufacturers may not be able to provide security patches if they do not know about their devices in the ecosystem as the consumers have not registered their devices). As IoT devices are often low costs, the manufacturers can be unwilling to provide security patches in a timely and regular manner as it is not cost effective for their business. Furthermore, end users may not have the skills (or the willingness) to register and manage the security settings. This requires the manufacturers should provide simple ways to achieve this, so that any consumer whether it is an 80 year old grandmother or an 8 year old child should be able to do this easily.

Achieving (a) and (b) does pose challenges; next we consider some practical mechanisms that can be employed by the government to achieve them.

(D) Q4-Q5: Government's role in a changing world

It is important that the government recognizes that it has an important role to play in the Cyber Security arena in the context of the provision and maintenance of a safe and trusted environment for activities and transactions in the digital ecosystem. In this context, in my view, there are some things that the government should do while at the same time it is equally important that there are certain things the government should not do.

What government should do

- I believe that government should establish and maintain mandatory *minimum* standards in cyber security, *particularly in the area of IoT technology products.* Government is often the single largest procurer of products and services in a country. In this capacity, government has a significant influence in getting manufacturers to modify standard security practices as well defining the security requirements. A government-defined minimum standard for cyber security (e.g.

demonstrated by a manufacturer prior to government procurement) can have a significant impact on ensuring that these products are available to everyone. The (initial) minimum standard will become the basis for further enhancements in the future. It will serve as a standard against which manufacturers can be made liable for delivering insecure products. A closely related issue is that government funded projects (using tax payer money) should be examples of excellence thereby government leading by example in the area of cyber security. (Note every security breach in government projects amplifies the failure of government in cyber security).

- Governments have long had an important role in maximizing social welfare (e.g. in regulating safety) whereas private sector providers do not have adequate incentives to do so. To deliver, it will need to coordinate and balance aspects of liability, transparency and privacy principles with the characteristics of specific industry sectors. The social welfare goals (whether free-standing or sectoral) will typically be some mix of safety and privacy. The former is likely to be dominant in transport (e.g. autonomous vehicles) while the latter may be more important in healthcare (e.g. medical devices). In the utilities and energy sector, such as smart devices, several goals can come into play; we do not want these devices in our homes to cause fires, or to leak personal data, or even to enable a foreign power to threaten to turn them off, to allow the utility to exploit market power, to make electricity theft easy, or to make it impossible to resolve disputes fairly.
- There is a role for government in helping the organizations to reduce their security vulnerabilities and compromises. In this regard, we have computer emergency response teams (CERTs) in many countries, so does Australia. However some accidents are more salient than others (e.g. critical infrastructures and services mentioned above), and voters will not be content for all fatal accidents to be valued equally.
    - This is clearly the case when it comes to essential and critical services and infrastructures that affect the national economy and society. We believe digital infrastructures should be included in this, as they form an essential part of provision of government services to the community. This will continue to increase even more in the future.
    - We believe it would be valuable for the government to establish a cyber security service targeted at SMEs, not only providing timely information to reduce security compromises and vulnerabilities but also help to develop *Cyber Security Expertise Hub for SMEs,* building cyber security expertise and capacity especially in the regional centers in Australia.

What government should not do

- Though there are certain digital infrastructures which are directly under government control, a large proportion of infrastructures (or even the majority of the infrastructures) is provided by the private sector. Even in these cases, there is a role for government to ensure that the digital infrastructures that affect citizens' daily lives are safe and trusted. Here it is critical that the government should not attempt to downgrade the security of digital infrastructures. This is vital for maintaining the trust and confidence of businesses and community to carry out their normal and business activities. It also helps to drive up the cost of the attackers which is part of the government's social welfare goal.

(E) Q6-Q11: Regulatory Environment for Cyber Security

First, it is worth noting that not all regulation comes from governments; the insurance industry plays its part, with insurance premiums and incentives. Indeed, governments sometimes justify intervention in protective cyber security on the grounds that they are the insurer of last resort. There is also some industry self-regulation, notably through standards bodies.

The goals of a cybersecurity regulator can be a mix of the following: ascertaining, agreeing, and harmonizing protection goals, setting standards, certifying standards achievement and enforcing compliance, reducing vulnerabilities and compromises, and reducing system externalities. Note the underlying principle of these individual goals is often to maximize social welfare by reducing risk.

Please see (D) above related to how government can help support the cyber security of consumer products. It is probably worth reiterating the opportunity for the government to address the supply chain security risk here. Creating a cyber security facility for SMEs (particularly in the regional areas) for conducting security self-assessments, understanding better the cyber security requirements and the vulnerabilities in the operating environments. Such a facility will help to achieve multiple objectives of supply chain security and SME security, both of which are critical for Australia. Please see also (G) below.

We briefly mention a few issues related to regulation due to changes in the nature of cyber security.

- As technology becomes embedded everywhere, software will play an ever-greater role in our lives. From autonomous cars to smart meters, and from embedded medical devices to smart cities, one environment after another will become software driven, and will start to behave in many ways like the software industry. There will be the good, the bad, and the ugly. The good will include not just greater economic efficiency but the ability to innovate rapidly on top of widely deployed platforms by writing applications that build on them. The bad will range from safety hazards caused by software bugs to monopolies that emerge as some of these applications and services become dominant. The ugly includes attacks. (Imagine cyberattacks on infrastructures in a smart city in Australia and the impact on its reputation worldwide).
- Hence we envisage the centre of gravity to shift from general regulation to sector-specific type regulation. That is, cybersecurity will not be regulated so much by privacy, national security, liability and transparency but more so by sectors such as cars, planes, medical devices, toys, etc. In many sectors, a whole range of aspects will need to be addressed, e.g. safety, privacy and security.
- Second, the regulation will need to be much more dynamic. At present, the regulation is largely static, consisting of pre-market testing according to standards that change slowly, sometimes if at all. Product recalls are rare, and feedback from post-market surveillance is slow, with a time constant of several years. In the future, regulation associated with safety and security will be much more dynamic; e.g. manufacturers of safety-critical devices will need to patch their systems often, just as phone and computing manufacturers do now.
- A strategic research challenge will be how we can make systems more sustainable. At present, we have enough difficulty creating and shipping patches for two-year-old mobile phones. How will we

continue to patch the vehicles we are designing today when they are 20 or 30 years old? How can we create toolchains, libraries, APIs and test environments that can be maintained not just for years but for decades? And how can this work within a learning system where we know that new attacks and vulnerabilities – and new types of hazard and vulnerability – will emerge, and we plan to monitor incidents and learn from them? Yes, machine learning systems have been advancing over the last few years but as of now *these machine learning systems themselves are susceptible to attacks*. This area of adversarial machine learning is one of the major strategic areas of research that falls in the intersection of cyber security and artificial intelligence. (See research projects in Advanced Cyber Security Engineering Research Centre (ACSRC) at the University of Newcastle website).

- A strategic educational challenge will be that security, privacy and safety will become intertwined, cultures and working practices will change. Safety engineers will have to learn adversarial thinking while security engineers will have to think more about usability and maintainability. At Newcastle, we are combining our strengths in cyber security and control systems engineering so that our students can get an appreciation of both security and safety/stability in cyber physical systems and industrial control systems.

(F) Q12-Q15: Cyber Security Professionals

- "Built-in" Cyber Security: Building cyber security functionalities at the time of design of products rather than as an add-on (usually as an after-thought) has been pretty much the bad practice in industry. For this to change, we need to have a change in the culture of designers and developers of products and systems. (I have had a direct first-hand knowledge of this as a Board Member in leading technology companies in the world). Yes, partly it is to do with education and training in cyber security of engineers and system and software developers. Partly it is also to do with senior executive in corporations not properly prioritizing cyber security (often it is the features which triumph over cyber security functionalities). Partly it is also the lack of demand or push from the customers and users and products and services. Of course, regulations (see (E) above) have an important role to play. *It is via regulation and procurement that government can influence the development of products with built-in security functionality at the time of design.*
- Trust in Supply Chain: As mentioned in (B) above, security in supply chain is a major issue that needs to be addressed both (i) from a technical perspective, as increasingly systems and products use many other subcomponents, and also (ii) from the SMEs perspective, who are often the manufacturers of components that are being used by larger systems and products. Hence government taking a proactive role in supply chain security has clear benefits both in the technical sense as well as in the business sense, as SMEs form a major proportion of businesses in the Australian economy. In order to instill trust in the supply chain, as already indicated earlier the government can set certain minimum security standards for its procurement thereby creating the need and market for secure products and components, leading to a wider adoption of secure products in the economy. We also recommend the government establishing security guidelines and standards in the IoT market in specific sectors such as medical devices, industrial control

systems and SCADA devices being used in the utility and energy sectors. Such proactive steps by government can help to instill greater trust in supply chain.

- Cyber Security Skills Shortage: As a Board Member in several leading technology companies in the world as well having been a member of Peak Government Advisory Groups in Cyber Security, it is clear to me that the shortage of cyber security skills is a worldwide phenomenon. Anecdotally, there is at least over 2 million job vacancies worldwide in cyber security. Building capacity in cyber security is via education and practical experience at tertiary level and it will take time. I do not believe there exists any shortcuts here. In fact, shortcuts will act as a detriment with the employment of poorly trained cyber security people in industry and government. There is a clear role for government in this space as they can influence the supply of cyber security professionals; a range of measures can be deployed such as creating targeted scholarships in cyber security at universities, and practical training and apprenticeships in cyber security at both TAFE and Universities, partnering with private industry to fund research and positions at Universities in specific cyber security areas (such as Cloud Security, IoT Security, Industrial Control Systems Security etc.) as well as providing targeted tax incentives to private companies to sponsor students and projects at Universities in cyber security etc.
- Another related and important aspect is to get a better understanding of the types of cyber security skills needed in Australia. Often this aspect gets overlooked when the total number of shortage is talked about. In some sense, the types of cyber security skills may be more important as it varies with the types of economies of different countries. There are different types of skills such as secure systems designers/developers, security architects, security analyst, security management, policy and regulation experts, etc. What is required is dependent on the type of economy one wants to grow, the market areas one wants to focus, the competencies and capabilities a country has and wants to develop etc.
- Given the technology scenery with cloud, IoT and big data, and the development of new services, applications and systems, ***we would emphasize the need for designers and developers of security products and systems (rather than just users).*** It is the development of new products and services that leads to growth of the economy and employment for Australia. Hence the ***focus on technical skills based on computing and engineering*** (such as large scale systems of systems, security devices, secure software, secure services and applications), ***combined with skills that can lead to the secure application and management of these technologies in different business sectors*** (e.g. finance, healthcare, defense etc.) ***together with skills involving prediction and management of business risks and social settings*** (e.g. trust models, social engineering etc.) ***are needed for Australia***
- Cyber Insurance: The market for cyber security insurance as the report indicates is still at an early stage in Australia. This is probably not surprising as the quantification of cyber security and the associated risk prediction models and loss analysis have not yet matured. However this is a potential area of growth which could be beneficial for Australia given our strength in the financial and actuarial services market.

(G) Q16 – Q21: Partnership with Private Sector

- Government can take some specific measures when it comes to partnering with the private sector in the protection of the digital ecosystem and increasing the bar for the attackers.
  - In the case of SMEs, there is an opportunity for the government to establish at least *minimum level security guidelines and templates that are sector specific a*nd work with the SMEs to ensure that these security measures have been enforced on a timely basis. As mentioned in (E) above, this cooperation with the SMEs can take the form of setting up specific cyber security facilities (especially in the regional areas) to assist the SMEs to conduct security assessments and enforcement of the sector specific security mechanisms. (Such a facility may form part of AusCyber whose charter currently seems to be more focused on promoting cyber security companies; the focus of the facility being proposed is more on the measures to improve the security of the SMEs and protection of their products and customers).
  - With respect to the general community and ordinary citizens, one standard approach is to partner with the major ISPs to ensure that the communications between the end user devices and the networks are secure as well as ensuring that the devices maintain a secure state (e.g. via anti-virus and security patches/updates). Here the government needs to work proactively with the ISPs to ensure up to date security measures are in place. There have been efforts in this area in the past, including amendments to the Telecommunication Act as well as code of conduct for ISPs etc. In this context, it is worth once again emphasizing that it is critically important not to introduce measures that weaken the security of digital infrastructures. This will have an adverse impact on the confidence and trust of the users and providers of online services, which will be a major detriment for the growth of the digital economy.
  - In the case of providers of critical infrastructures and services, the role of government is to ensure that there is adequate sharing of security related information between these providers and the government agencies. I am well aware that the government has had various mechanisms and processes in place for this. In this regard, in the past, I have been a member of ITSEAG (IT Security Expert Advisory Group under the auspices of AG and BCDE) as well as Trusted Information Sharing Network (TISN). Furthermore there have been some sector specific committees, in particular, I was involved in a specific committee (a few years back) concerned with SCADA security, which was highly productive developing a comprehensive security guidelines and best practice jointly with the suppliers, contractors and users of SCADA equipment. It would be worthwhile to revive such strategic committees at *sector specific level.* E.g. develop and communicate guidelines for industrial control systems security best practices for rapid deployment and use.

- Critical Infrastructures and Services: In addition to the usual critical infrastructures such as utilities, transportation systems and energy and telecommunications networks, there is a need to include digital infrastructures (such as data centres) in this category of essential critical services. With the ever increasing use of data in many different applications and decision making services, data has become the new currency and digital infrastructures that handle data will require

stronger cyber defenses. In fact, we believe it is critical to develop new data centric security architectures and solutions that will underpin many of new technology services and applications of the future (leading to a competitive advantage for Australia in some niche markets).

- Funding Model: As protection of digital infrastructures and ecosystem is an integral part the national agenda for economic growth, this must form a core part of government strategic policy priorities, and hence specific strategic funds must be allocated within the government's budget from public resources (e.g. Dept. of Industry and Innovation and Dept. of Infrastructures).

(H) Q22 – Q25: Cyber Awareness

- Consumer Choices: When it comes to consumer choices and user behavior, there is no one-size-fits-all solution. Effective influencing requires more than simply informing people about what they should and should not do: they need, first of all, to accept that the information is relevant, secondly, understand how they ought to respond, and thirdly, be willing to do this in the face of many other demands. Having said this, cyber awareness is still generally low in the community despite the publicity about the data breaches and attacks in the recent times. When it comes to decision making about the purchase of many consumer products, factors other than cyber security tend to play a major role. This is likely to be the case in the case of IoT products. The situation is further aggravated as many consumer IoT devices do not have security functionality.
- To understand the cybersecurity implications of the widespread deployment of connected devices, the public will need to be better educated and more involved. The goal should be to achieve security by default in all connected devices and to ensure that the consumer and integrator alike know what security capabilities are, or are not, contained in these devices. Here, as mentioned earlier, it will be valuable for government to establish sector specific minimum security standards and guidelines.
- Increased consumer focus on cyber security will clearly benefit Australian businesses as it will provide the needed impetus to develop cyber security products.
- Most certainly would be keen to see cyber security features prioritized in systems and services. In fact, this has been one of the main goals of several of the industry Boards that I have been a member of. This will certainly help to improve the market offerings in cyber security, which in turn can make the digital ecosystem safer.
- There have been various cyber security awareness efforts in different countries some more successful than others (at least for a period of time). Here are some popular ones that come to my mind.
    - GetSafeOnline Campaign in the UK focusing on users at home and in businesses. At its core, the message emphasizes to individuals that they have the responsibility for getting safe online. The campaign offers a comprehensive repository of information on threats and how-to advice on protecting oneself and one's enterprise. The charge, however, is on individuals to make use of this information and properly apply it to their context.

- Another one from the UK, Cyber Streetwise Campaign, probably a better one in terms of causing a behavioural change by providing tips and advice on how to improve online security, using a positive message (''In short, the weakest links in the cyber security chain are you and me''). Advises to adopt five basic measures to boost their security, such as using strong, memorable passwords, installing antivirus software on all devices, checking privacy settings on social media, checking the security of online retailers before loading card details, and patching systems as soon as updates are available.
- The awareness campaigns need to reflect cultural aspects; for instance, in countries like the UK, individual responsibility is emphasized, whereas in other countries in Africa, a more collectivist approach is used in terms of users' relationships and social group memberships (e.g. parents), as well as the need to fulfil duties and obligation.

(I) Other Issues

In this section, we would like to raise a couple of additional issues:

- We believe there is a clear need to boost R&D in Cyber Security in Australia and this should form part of the 2020 Cyber Security Strategy, funded via both government strategic initiatives as well as via public private partnerships. Though cyber security issues arise in several different areas ase mentioned above, we would like to single out the area of Internet of Things Security as a key strategic area of focus for Australia. The growth of network connected devices, systems and services comprising IoT creates immense opportunities and benefits for our society. In particular, 5G networks with IoT impacts on society will be immense with applications in a range of sectors such as healthcare, transportation, smart cities and industrial control systems, enabling digital economy on a much larger scale. The areas such as IoT and Industrial Control Systems Security require fundamental research and development not just to develop solutions that continue to foster innovation, but also to build in opportunities for reducing the risk involved with ubiquitous connectivity. The private sector generally funds and focuses on near-term research and on transitioning successful research (from any source) into commercial products. Government funding of long-term, high-risk research and of mission-specific R&D thus remains critically important. Funding for creating inherently secure technology, products, systems, and environments in Australia is in comparison relatively small. The government should invest in fundamental cyber R&D that will foster the development of inherently secure, defensible, and resilient/recoverable systems. The private sector should work with the government to ensure that the results of this research are readily usable in improving technologies, products, and services. In this regard, the Advanced Cyber Security Engineering Research Centre at Newcastle has specific research focus in the areas of IoT Security with applications to Industrial Control Systems and Healthcare Security.
- We believe there is an even greater need to enhance collaboration between government agencies, industry and academia. (I recall writing a Draft Paper in 2010 for PM&C prior outlining such a framework prior to the creation of CSOC). Following CSOC establishment and then in 2013

with the creation of ACSC have led to increased interactions between the various government agencies as well as with sections of the industry. This has been a highly positive outcome. However the linkages with academics have not happened in any meaningful manner. I believe, as part of the Cyber Security Strategy 2020, it would be beneficial to create mechanisms for appropriate academics[i] to be involved with organizations such as the ACSC.

Concluding Remarks

I am thankful to the Australian Government for this opportunity to provide inputs to 2020 Cyber Security Strategy for Australia.

I hope the comments and suggestions given here will be of some help to the Dept. of Home Affairs in its deliberations. I will be most happy to elaborate on any of these issues mentioned here if required.

Best Regards

Vijay Varadharajan FIEE, FACS, FIEAust, FBCS, FIMA, FIETE

Global Innovation Chair Professor in Cyber Security, Australia
Director of Advanced Cyber Security Engineering Research Centre (ACSRC)
The University of Newcastle, Australia
Email: [redacted] T: [redacted]
Webpage: https://www.newcastle.edu.au/research-and-innovation/centre/advanced-cyber-security-research-centre/people/professor-vijay-varadharajan-biography

[i] E.g. With relevant expertise in cyber security and recognized experience in industry, and security strategy & policies.