ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, Illinois 60173, USA
Telephone: +1.847.253.1545
isaca.org | E-mail: info@isaca.org

31 October 2019

The Hon Peter Dutton MP
Minister for Home Affairs
PO Box 6022
Parliament House
Canberra ACT 2600

Dear Minister Dutton:

Thank you for the opportunity to respond to the Australian Government's Call for Views on Australia's 2020 Cyber Security Strategy. ISACA's global community, as well as the more than 4,000 ISACA members within Australia, is grateful for the opportunity to provide its views and continued its ongoing support of the world-leading efforts of Australia in developing and evolving a forward-focused and comprehensive national cyber security strategy. In ISACA's response to the Government's Call for Views, we have chosen to address those questions that ISACA believe lie squarely within our fields of interest and expertise.

Since the Government's 2016 launch of a national Cyber Security Strategy, great progress has been made against the goals set in the Strategy. The opening of the Australian Cyber Security Centre within the Signals Directorate, with the Centre given the charge of serving as a central source for cyber expertise throughout the Government was an enormous milestone—but far from the only one.

Establishing Joint Cyber Security Centres throughout Australia to enhance interactions between the public, private, and academic sectors is another key stride forward that has been made, as has demonstrating Australia's leadership within the international cyber security community through the appointment of an Ambassador for Cyber Affairs.

Perhaps most important has been the Government's focus on the future; demonstrating its commitment to tomorrow's cyber security leaders through the creation of Academic Centres of Cyber Security Excellence, among other critical educational endeavours. All of these advances were possible because of untiring commitment to the implementation of the elements of the 2016 Cyber Security Strategy, and national recognition of the importance of cyber security across all facets of life, business, and communications.

Regrettably, however, the threat environment in which the Government seeks to build the 2020 Cyber Security Strategy has evolved as well. As the Government works to write the next chapter in Australia's Cyber Security Strategy, it does so within cyber security and cyber attack landscapes that have seen incidents impact citizens, private and public sector organisations, and nationally important systems. It is not merely evolution of these landscapes, however; it is expansion as well. These past few years have seen attacks grow in impact and scope as the 'cost threshold' for being a malicious actor has decreased, and as State actors are increasingly playing a role within the attack landscape.

Globally, cyber security remains a priority to address increases in cybercrime and, in some instances, cyberwarfare. Factors contributing to the need for improved cyber security include ubiquitous broadband, IT-centric businesses and industries, and societal and social stratification of skills in information and cyber

security. To improve cyber security, many governments and institutions have launched cybersecurity initiatives, ranging from guidance, through standardisation, to comprehensive legislation and regulation.

Worldwide, there is a significant global shortage of skilled cybersecurity professionals, and Australia is no exception to this shortage. ISACA has made a firm commitment to proactively address this skills crisis and deliver for cybersecurity professionals what it has accomplished (and will continue to do) for audit, control, governance, and information and cyber security professionals for the past half-century.

The ISACA community in Australia believes it can render assistance to the Government as it seeks to build the 2020 Cyber Security Strategy by:

- Supporting the Government's efforts to address Australia's cyber security, audit and governance skill needs for security professionals, non-professionals and consumers alike.
- Sharing proven information and technology governance guidance and offerings with Australia's public and private sectors, with the goal of organisational- and eventually ecosystem-level cyber security improvement.
- Looking to the future of cyber security, particularly in the context of emerging technologies, assessing risk, and providing advice, training and research about how to increase Australia's overall cyber resilience.

ISACA believes assistance in the above points would enable the Government to better protect Australia, including what are currently considered critical infrastructures, as well as other infrastructures that may take on similar critical significance in the future. The ISACA community in Australia would also provide ongoing advice and guidance on technological and international developments to support the Government's efforts as an international leader in cyber security.

ISACA believes the development of Australia's 2020 Cyber Security Strategy is another crucial step in the journey by the Government to strengthen trust in and value from public and private sector information systems. ISACA stands ready to offer its global network of highly experienced and certified volunteers—backed by professional staff—to assist the Government in any and all appropriate future endeavours, including work with Australia's universities and training providers in delivering cyber security training, certifications and research.

ISACA would also like to advise the Government that Ms Jo Stewart Rattray [redacted] and Mr Tony Hayes [redacted] are ISACA leaders in Australia who are available to provide additional information briefings and/or coordination to assist Government officials with their endeavours as needed.

Respectfully submitted,

[redacted]

David Samuelson
ISACA Chief Executive Officer

About ISACA
Now in its 50th anniversary year, ISACA® is a global association encompassing the strong local communities built by our more than 140,000 members, including the more than 4,000 professionals working throughout Australia. ISACA equips professionals with the knowledge, credentials, education and networks to advance their careers and transform their organizations. Together with its enterprise performance improvement subsidiary CMMI® Institute, ISACA leverages the expertise of its international communities in information and cyber security, governance, assurance, risk and innovation to help advance innovation through technology.

ISACA

The Australian Government's 2020 Cyber Security Strategy Call for Views

ISACA Responses

1) What is your view of the cyber threat environment? What threats should Government be focusing on?

ISACA's Australian community, comprised of members across the breadth of the nation's public and private sectors, has seen firsthand that the cyber threat environment of today is not the same as that of only a few years ago. The landscape has evolved dramatically, and has done so in a manner that has increased levels of concern for the security of critical infrastructure systems, the personal information of citizens, and the very integrity of Australia's democratic processes.

In these three key areas, Government is not faced with an either/or choice; to ensure Australia's future cyber security, Government must make all three of these areas—as well as ongoing efforts as an international leader in cyber norms development—of primary and critical importance. Cyber security against threats is best addressed through a robust and comprehensive ecosystem of individuals, organisations, and institutions; all must improve for the ecosystem to function at it utmost within the cyber threat environment.

2) Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

Yes. The Government's understanding of the current landscape for responsibility in the managing of cyber risks in the economy is accurate. ISACA would respectfully point out, however, that because the general citizenry is tasked with responsibility for dealing with cyber security risk, additional awareness-raising efforts amongst the populace would be invaluable in the management of personal cyber security risk.

3) Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

One of the questions in this Call for Views asks about 'building in' cyber security within digital goods and services, and ISACA sees this as related to this question. While 'building in' cyber security may place an additional responsibility upon the shoulders of business, it is nonetheless a shifting of responsibility that ISACA believes is in the best economic and security interests of the Government.

Information and technology governance should not be sacrificed for speed-to-market. The end user should not be expected to be the responsible party for something they had

little or no role in creating or developing; basic consumer research is an insufficient substitute for thorough and due diligence in governance efforts.

One change worth considering as a way to support efforts to increase the presence of information and technology governance (while still encouraging a strong digital/cognitive and cyber secure economy) is the adherence to minimum standards for information and technology governance. This could take many forms, but should ideally be developed between the public and private sectors, as well as the technology certifications and standards development communities, to ensure that the needs of business, government and the consumer are met and that the responsibility for the management of cyber risk begins at the inception of a product or service's lifecycle—not with the end-user licensing agreement.

Just as the European Union's General Data Protection Regulations (GDPR) as well as Australia's own Privacy Principles have given rise to a new cohort of data processing professionals, Australia could serve as the starting point for embedding information and technology governance professionals within products and services lifecycles. Additionally, certifications like ISACA's Certification in the Governance of Enterprise IT (CGEIT, which focuses on information and technology governance) and other similar credentials within the governance space could become preferred or requisite credentials for professionals charged with managing cyber risk throughout product or service lifecycles.

4) **What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?**

Government should be an enabler of solutions, rather than the entity directly addressing threats to non-governmental institutions and businesses in Australia. To this end, Government should explore approaches that lessen the threat landscape proactively, rather than increase its role in a reactive response.

For example, training and awareness of risk are fundamental to driving shifts in the perception of cyber risk, for both organisations and individuals. ISACA's experience, in both Australia and globally, has been that that a key driver in lessening the threat landscape is a professional cadre adherent to certain levels of professional qualifications or certifications in fields such as information and cyber security, as well as risk. A focus by the Government on requiring that front-line cyber security personnel possess certifications from recognised information and cyber security organisations, such as ISACA's Cybersecurity Nexus (CSX) family of credentials, is a proactive step forward in addressing cyber risk.

While adherence to such standards of qualification is valuable for individual professionals, it is important that holding those professionals to higher standards occurs within organisational infrastructures that complement their expertise. Mandating that

the senior levels of organisations possess adequate appreciation for and demonstrated expertise in technology and information governance (through acquisition of credentials) ensures that appropriate measures are in place to protect both that organisation and the greater digital/cognitive economic and security ecosystems. To complement the efforts made to hold professionals to higher standards of excellence, employing business frameworks such as ISACA's COBIT (Control Objectives for Information and Related Technologies) and other similar constructs provide additional support to the business processes underpinning the governance and management of an organisation's data, information, and technologies.

Addressing serious cyber threats to Australia's institutions and businesses is also an activity that cannot stop at the border. In the past, the Government has worked with nations as diverse as Israel, Singapore, and several of the nation's ASEAN neighbors; these are efforts that should continue to be built upon to address cyber threats that arise from outside the nation. Such borderless emphasis on providing appropriate and comprehensive cyber security also plays a role in lessening the threat landscape, and it is critical that the Government's commitment to addressing cyber threats to the public and private sectors inside Australia be matched by an equal commitment to addressing cyber risk from actors residing outside the nation's borders.

5) **How can Government maintain trust from the Australian community when using its cyber security capabilities?**

The Government must retain the trust of the Australian people when it exercises its cyber security capabilities—and the people must trust that those capabilities are utilised responsibly and appropriately. Sacrificing personal privacy for security, for instance, is counterproductive to maintaining Australia's trust of its Government's cyber security efforts. While concerns for maintaining trust may create difficulties for Government when working within existing legislative frameworks, it is nonetheless a worthwhile pursuit. One example of this are the ongoing legal and industry concerns regarding the provisions of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act of 2018. There is already discussion of revisiting the 2018 Act to address issues of uncertainty within the business sector (particularly among such organizations as cloud service providers and IT product developers, among other businesses using encryption as a core element of their respective security and privacy frameworks). These are not easy questions, and there will not be easy answers—but to maintain trust, the Government must continue to work with all involved parties and sectors to arrive at mutually acceptable resolutions.

That is not to say, however, that creative remedies that balance national security while maintaining trust cannot be found. The Australian Cyber Security Centre releases public warnings to vulnerable organisations, but response is not mandatory; that can be changed, with fines incurred for noncompliance with those warnings. In this way,

adherence to these warnings becomes part of normal operations for organisations and the Government gains at least a temporary revenue stream from noncompliance.

However, even before such a change could be made, there are several elements to consider. First and foremost, organisations must be aware of the Centre's offerings regarding these public warnings; improved efforts must be made in this regard before any consideration of non-compliance repercussions can be considered. Second, to accomplish such awareness-building, the Government would ideally work closely with ASIC to ensure that awareness of the Centre's offerings was a condition of organizational registration. Finally, there are potential changes to the Corporations Act that may need to occur. These are not insurmountable obstacles, however, and should be considered part of overall efforts to ensure public policy keeps pace with technology's evolution.

Concerns regarding the Government's ability to respond swiftly in emergency situations can be addressed in a similarly creative manner. Granting appropriately credentialled and experienced operational staff the ability to exercise executive-level decision-making when cyber security incidents reach a specific level could be one approach; creating rapid-response cross-Government teams of cyber security incidence response professionals empowered to act in a similar manner when emergency-level incidents occur is another. However, in the creation of these teams or in the 'combat promotion' of operational staff during a cyber security incident, care must be given to ensure that the professionals involved meet the highest levels of demonstrated expertise in information and cyber security and ideally possess the certifications and other qualifications that evidence that.

6) What customer protections should apply to the security of cyber goods and services?

In the earlier response to Question 3, we noted that the 'baking in' of security and consumer protections is a critical step the government can take to ensuring the security of cyber goods and services throughout their lifecycle. ISACA stands by that earlier assertion. Whilst the Government's stated goal of delivering long-term societal benefits without overly burdening industry with additional costs is admirable, it may not be entirely realistic. Though care should be exercised to ensure that innovation within Australia's cyber goods and services providers is not stifled in any way, care should also be exercised in the shifting of at least some of the responsibility for the security of cyber goods and services to industry. One question worthy of consideration is the potential application of existing legislation, such as the 2010 Competition and Consumer Act, to hold technology providers to account for security vulnerabilities, poor designs, or product failures, and to provide consumers with notice regarding the deployment of poorly-secured products or services; this could be a way in which to adapt existing legislative frameworks to an evolving technology landscape.

As the Government has noted in its Case Study of the EU's "Network and Information Security Directive" (NISD), there is the possibility of both proactive and reactive supervision for certain sectors; variations on the NISD approach could yield the results the Government is looking for—a prosperous and secure Australian digital economy that still ensures positive benefits for Australia's citizenry.

7) **What role can Government and industry play in supporting the cyber security of consumers?**

Perhaps the easiest role the Government and industry in Australia can play is the role of educators. Whilst some success has been encountered in the past, through initiatives such as the Government's "StaySafeOnline" efforts, this success must be balanced against the consideration that such efforts have largely been limited to subscribers and advocates. This is, to be sure, exceptional work, and worthy of recognition—but it is a step in a journey, and should be seen as progress, but not a complete solution.

Joint public-private initiatives to increase consumer awareness of appropriate cyber security measures that can be easily used by individuals to protect themselves are one possible action that can be undertaken. Similarly, the inclusion of cyber security curriculum within the primary and secondary education levels to teach consumer cyber security to young students is certainly another path to explore, as is the addition of security considerations within coding course curricula at both the pre-university and university levels. Credentials such as ISACA's CSX Fundamentals (CSX-F), which explores the fundamentals of cyber security, could become included in such curricula, providing students with additional achievements to build upon as they pursue post-secondary and even post-tertiary educational pursuits.

8) **How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?**

Though the efforts by the Government and industry to educate consumers outlined in ISACA's response to Question 7 would be a welcome step forward, they should not be the only steps taken. Mandating that industry adhere to minimum standards of cyber security protections—protections that do not stifle innovation, but still protect the consumer, be that an individual, a business, or even the Government itself—is a course worth pursuing.

The Government may also wish to consider including entities engaged in vocational education and training as a vehicle for ensuring Australia's cyber security workforce possess appropriate levels of knowledge and expertise. TAFE-SA (Technical and Further Education-South Australia), already offers a Cyber Security Traineeship program, and there are other similar programs throughout the nation; an emphasis on supporting and perhaps expanding vocational education and training could also be of benefit.

Also—as was noted in ISACA's response to Question 3—it is imperative that industry and the Government work together to arrive at a consensus regarding minimum standards for information and technology governance with respect to the cyber security of digital/cognitive offerings. Additionally, benchmarking governance and cyber security capabilities within an organisation and across industries provides continual monitoring and measuring of cyber capabilities throughout an economic ecosystem, ensuring that the security, quality and effectiveness of cyber security efforts is always functioning at the highest levels possible.

These efforts are incomplete, however, without well-trained, high-quality professionals to support them. ISACA believes that the widespread adoption of a cyber security culture rooted in a mutual commitment to sound technology governance is a goal of pivotal significance. This culture should permeate all Government agencies and the private sector, as well as the supply chains that service them. Key steps forward include:

- Creating credentials, badging or "concentrations" in key cybersecurity topic areas tailored to meet the needs of the Government's cyber workforce and key private sector segments (i.e., critical infrastructure), leveraging current commercially-available security credentials
- Educating all Federal Government employees (executives, non-technical personnel, etc.) in cybersecurity best practices based upon their occupational needs and the risks they face
- Architecting opportunities and projects that create and foster a sustainable cybersecurity culture grounded in technology governance at the enterprise level
- Recruiting new, qualified IT personnel, as well as cross-training and re-skilling current personnel, and fostering a strong educational pipeline to continue to supply highly skilled cybersecurity personnel to the public and private sector workforces far into the future.

Steps such as these are of paramount importance, for they provide both security and economic benefits, but more steps can be taken. Such steps could include, but are far from limited to: financial or other incentives to support training and skills development; recognition of internationally accepted cybersecurity certifications in a manner similar to the way that the Information Registered Assessors Program (IRAP) recognises international certifications (including ISACA's own Certified Information Systems Auditor [CISA], Certified Information Security Manager [CISM], and Certified in Risk and Information Systems Control [CRISC] certifications) as pre-requisites; and perhaps even a renewed focus within the Government's procurement activities to make extensive use of Australia's small- to medium-enterprises, thus encouraging this crucial economic sector to, in turn, up-skill and re-skill their IT workforces.

Within Australia's burgeoning digital and cognitive economies, no private sector enterprise nor public sector agency is an island unto itself; contracts, regulations, registrations and countless other intersections inextricably link them together. The adoption of a robust and systemic cyber security culture within a high-quality

professional corps is a crucial step forward in ensuring Australia's continued prosperity, growth and security whilst still increasing the quality and effectiveness of cyber security and digital/cognitive offerings.

9) **Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?**

It is ISACA's considered opinion that devolving or outsourcing Government functions to become functions of the private sector is perhaps not the best course of action. Instead, ISACA would respectfully suggest that Government focus more on creating public-private partnerships, so that it retains a voice in the evolutions of those functions. The Government of Australia has one concern—and one concern only—top-of-mind: the security, prosperity and welfare of its nation. The private sector, by contrast, must answer to shareholders and the market; this is not reassuring when issues of national concern, of impact to all Australians, are at stake. There are lessons to be learned from industry, to be sure, but the Government should work with the private sector to mutually improve one another, in partnership. Ceding functions to the private sector—safely or not—is not as beneficial a choice for the Government.

10) **Is the regulatory environment for cyber security appropriate? Why or why not?**

Whilst the Government has taken some steps in past years to ensure Australia's regulatory environment keeps pace with changes in cyber security and technology, there is still much left to accomplish. Australia's regulatory environment—like many other such national regulatory environments the world over—is still wrestling with issues that impede Government's ability to have public policy keep pace with technological evolution, particularly in areas such as encryption and privacy, among others.

As the impacts of the GDPR (and, to a lesser extent, the California Consumer Protection Act, or CCPA) continue to be key issues of consideration among regulatory bodies in nations around the world, there will likely be discussion in Australia regarding enhancements to the Government's existing privacy-focused legislation, and whether it can be aligned to measures such as the GDPR and CCPA. If such discussions led to regulatory action and eventual implementation by data holders, this could be instrumental in reducing data privacy exposures in the event of cyber security compromises.

ISACA's belief is that an appropriate regulatory environment for cyber security is one that is anticipatory and proactive. Rather than being reactive to issues that arise, the Government, industry, and the academic sector could be exploring issues of regulatory concern while emerging technologies are still in their infancy, rather than when they arrive in the marketplace. This approach not only ensures the needs of industry and government are met but has the potential to provide benefits to consumers as well.

11) What specific market incentives or regulatory changes should Government consider?

The Government could consider the provision of tax incentives, rebates, reduced fees, or similar enhancements to organisations that have demonstrated appropriate levels of cyber maturity. In addition, the Government could recognise those organisations that have achieved consistently high levels of cyber maturity over time, perhaps with some sort of recognition or accolade that certifies that organisation's commitment to cyber security over time and, by extension, the trustworthiness of the organisation in matters of cyber security maturity.

Last year, ISACA was pleased to have had the opportunity to participate in a consultation put forth by the Australian Prudential Regulatory Authority (APRA) regarding APRA's proposals for the new Prudential Standard CPS 234 Information Security. At that time, ISACA's response indicated that increased costs for compliance be perceived as investments rather than incurrences. It was ISACA's contention that, by strengthening risk and data management and security practices throughout Australia's financial sector, ARPA's efforts would strengthen yet another pillar within Australia's digital economy, making both the economy and the sector stronger, more secure, and more resilient.

ISACA's consultation response to ARPA also suggested a 'stepped' approach to implementation of the Prudential Standard, an approach that would provide adequate timelines for all organisations involved, ensuring compliance without overburdening the organisations, and minimising the immediate impact of compliance costs. Such an approach, ISACA believes, might be of benefit when the Government is considering market incentives or regulatory changes across the breadth of Australia's private sector.

In the past, initiatives and programs such as Austcyber have aided cyber-focused startups to gain funding to bring their ideas and offerings forward. At present, future funding to support Austcyber is uncertain; it is ISACA's considered opinion that worthwhile endeavours such as these retain continued support, to better expand the marketplace of cyber-focused companies within Australia.

12) What needs to be done so that cyber security is 'built in' to digital goods and services?

In the response to Question 3 in this Call for Views, it was noted that ISACA believes that it is in the best economic and security interests of the Government to shift some of the responsibility for 'building in' cyber security to business and industry, while taking care not to stifle innovation. Similarly, ISACA believes that information and technology governance can and should be a core component of the development of any digital product, service or solution. As ISACA suggested earlier, adherence to minimum

standards for such governance is a starting point, and those standards should be developed by the Government in concert with industry.

ISACA also contends that the environment must be conducive to 'building in' cyber security into digital goods and services. This means workforces adhering to a certain standard of expertise within cyber security and/or information and technology governance, and ideally possessing certifications, such as ISACA's CGEIT or CSX-P or other similar credentials, that demonstrate that adherence.

It is not just the professionals, however, that should be held to standards of expertise in cyber security and information and technology governance; it is organisational leadership as well. Throughout Australia's private sector, there has been progress in recent years in ensuring that Boards and C-suite leaders recognise the need for cyber security to be 'built in' to digital goods and services. That progress, however, remains incomplete; there is still room for improvement; despite this being a topic of some interest in recent years, there is still a significant cohort of Board members who remain uncertain of what information and technology governance really is, or why it is needed. Ensuring that all boards and organisational leadership teams possess expertise in areas such as cyber security and the governance of information and technology is a goal worthy of pursuit by both the Government and industry.

13) How could we approach instilling better trust in ICT supply chains?

In previous Question responses within this Call for Views, ISACA has noted that it views cyber security, governance, and trust as functions best improved within an ecosystem, in which individuals, organisations, industries, the Government, and the regulatory and cyber threat landscapes facing these entities is taken into consideration. ISACA sees ICT supply chains as being no different; their very existence necessitates an ecosystem approach to improving security. A supply chain can only be as strong as its weakest link; ensuring that all links in the chain are strong automatically improves trust. As ISACA has noted in prior Question responses, emphasising a strong, high-quality workforce, equipped with the right tools and credentials, functioning within organisations committed to giving cyber security concerns the primary levels of concern they deserve, is the kind of approach that must be taken in order to instill trust not only in each discrete link in ICT supply chains, but along the length of the chain as well. A key element in the securing of these chains is the assurance of cyber security maturity within third parties. ISACA's CISA credential supports the performance of this, and APRA's CPS234 has third party assurance as a key component. Other sectors could follow APRA's example to uplift the cyber security maturity of their respective ecosystems.

14) **How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?**

In ISACA's response to Question 8 of the Call for Views, a number of key steps that could be taken to enhance the widespread adoption of a cybersecurity culture were outlined, among them appropriate credentialing and certification; education of cyber security and non-technical personnel in cyber security best practices; fostering a strong educational pipeline that includes an emphasis on employee re- and up-skilling and training.

There is also a significant need to encourage women to enter into the cyber security workforce; ISACA's 2019 State of Cybersecurity Report noted that 89 percent of respondents indicated that there are more men than women in cyber security roles within their organization. ISACA's SheLeadsTech program, which seeks to increase the representation of women in technology leadership roles and the technology workforce, has already met with great success in Australia and abroad. As the findings in the Report indicate, however, much work remains to be accomplished in ensuring that workplaces and workforces are more diverse and inclusive, particularly with respect to gender.

15) **Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?**

In the Call for Views, the Government notes that "*Difficulties in quantifying the risks and potential losses from future cyber incidents could be a barrier to growth in this area.*" This, ISACA believes, is one of several barriers to continued, robust growth of Australia's cyber insurance market. Concerns regarding systemic events that could bankrupt an insurer's business have not gone away; large-scale cyber attacks and ransomware incidents do nothing to assuage those fears.

Like other markets around the world, Australia's cyber insurance community continues to wrestle with where to 'place' cyber—as a stand-alone product or included within other coverages such as general liability or property. It will be critical for the Government to continue to work with the insurance community to explore what, if any, regulatory remedies there may be to definitively 'place' cyber insurance where it is optimally suited. Similarly, these solutions and remedies must be found for the intersection of cyber insurance and emerging technologies, particularly AI and machine learning technologies.

Several States in the United States, the entire European Union, and several governments in Australia have all put measures in place requiring the purchase of cyber insurance. This is certainly a position the Government could take, but it is ISACA's contention that any such endeavour be undertaken jointly with Australia's insurance community leadership to ensure the best possible environment for continued growth of the national cyber insurance market. Additionally, due to the diversity of coverages provided by cyber insurance—and the equally diverse business sectors it insures—it would be

beneficial for the Government to not only include the leadership of Australia's insurance community in any efforts to grow the national cyber insurance market, but leaders from across the breadth of the private sector as well.

16) **How can high-volume, low-sophistication malicious activity targeting Australia be reduced?**

In ISACA's response to Question 4 of this Call for Views, there were two areas touched upon that hold great promise in reducing the targeting of Australia and its citizens with high-volume, low-sophistication malicious activity: the Government's work on the international stage in shaping cyber norms, and increased emphasis on training and awareness among cyber professionals and nonprofessionals alike.

The Call for Views discussed mid-level capabilities within cyber security efforts, and ISACA believes that these measures—particularly efforts to both gather and share information—are also vital tools in ensuring adequate cyber security for the nation and its citizenry. Knowledge is a powerful tool within cyber security. A more cyber-aware populace will be better able to identify and avoid malicious activity. Increased training in cyber security fundamentals for cyber professionals and nonprofessionals will decrease similar activity in the workplace. Sharing information within and across public and private sectors and industries will be of benefit to Australia's digital marketplace ecosystem. Working with national partners in the ASEAN region and abroad enables the Government to gather timely, critical information on outside malicious actors targeting Australia. Any one of these actions is important and can be impactful; done in concert, they synergistically enhance one another, greatly reducing Australia's risk of malicious activity.

17) **What changes can Government make to create a hostile environment for malicious cyber actors?**

It is ISACA's considered opinion that, while the steps outlined in the response to Question 16 are important, there is yet another step that Government itself can take to create an environment hostile to malicious cyber actors: engaging in an unceasing commitment to remain proactive in its cyber security efforts.

For years, the Government's work with the international law enforcement community has played a critical role in ensuring Australia's security. Whilst that role has evolved with the rise of cyber security, it must continue to evolve, expand, and deepen. As was mentioned before: knowledge is a powerful tool in cyber security. Foreknowledge—of state-sponsored malicious or organized criminal activity, or simply of upticks in ransomware attacks—is an even more powerful tool, for it provides the ability to prevent attacks rather than respond to them. When such efforts are combined with an

emphasis on increased cyber security and attack resilience within organizations, industries and networks, Australia is the more secure for those actions.

18) **How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?**

The Government, in ISACA's considered opinion, has already demonstrated the best way to answer this question—and it has done so with deeds, not words. Industry has worked with the Government in the past to proactively identify, prevent and remediate risk on essential networks; this collaborative approach is of paramount importance. What comes next is the logical expansion and deepening of those efforts. It will take both private entities and the Government to define "essential" private networks, and to do so in a manner that is organic and anticipates an evolution of that definition. Likewise, it will take both parties to arrive at mutually acceptable risk remediation strategies and approaches that do not sacrifice security for prosperity—or vice versa.

ISACA believes it is too early to discuss cost recovery and similar matters. Issues that should occupy primary importance are those surrounding what should be considered "essential" networks; what those networks should look like in terms of trained, high quality personnel, adherence to standards of expertise, and leadership versed in either information and technology governance or cyber security; and how best to implement compliance requirements that emphasise growth, but not at the expense of security.

19) **What private networks should be considered critical systems that need stronger cyber defences?**

There is a defined need to secure the usual critical infrastructures and systems that are largely in private hands, such as the energy, food, finance, government, and other sectors that are vital to the provision of essential products and services.

Whilst there is a focus on the protection of finance as a critical system, this focus does not necessarily extend to the protection of commerce. Though the distinction is subtle, there remains great impact in the difference. Government does not function in a vacuum; there is a constant web of interactions that bring private sector providers of products, services and solutions into contact with the public sector. Whatever impacts one has the potential to impact the other, to the detriment of both. For this reason, the expansion of the 'finance' and 'government' sectors that the Government currently strives to protect is an undertaking worth considering. We also believe the Government should consider the 'ripple effects' those sectors have on other areas through supply chain relationships.

In an interconnected global digital economy, definitions of critical systems require adjustment—and perhaps a bit of flexibility as well. Our interconnected world has

brought extraordinary advances; it has also brought with it the need to cast as wide a net as possible when considering cyber security for critical systems and infrastructures.

20) What funding models should Government explore for any additional protections provided to the community?

ISACA believes this to be an area of expertise better commented on organisations more focused on funding models and economic endeavours.

21) What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

It is a long-held belief—correct or not—that the public and private sectors often hold differing emphases and priorities, and operate at differing speeds. Whilst these may be constraints to information sharing, it may behoove the Government to learn from the actions of industry, and from industry to learn from the actions of the Government.

In ISACA's response to Question 5 of this Call for Views, we emphasised the important and ongoing efforts of the Australian Cyber Security Centre in releasing public warnings to vulnerable organization. It was also noted that such notifications could become mandatory, with fines incurred for noncompliance.

However, deriving revenue from a relationship does not have to be limited to the Government; industry can and should profit from the information sharing relationship it has with the public sector. Companies actively participate with whitehat hackers through 'bug bounty' programs that identify problems with products, services, and solutions prior to that offering's release. As further evidence of proactive security within the business ecosystem, some Australian-grown Software-as-a-Service companies are deploying "Vulnerability Disclosure Policies" whereby they voluntarily alert their clients of internally detected vulnerabilities or bugs which may impact their client.

Government could take a page from industry in this regard, providing rewards of some monetary value to industry (i.e., reduced business-related fees, lowered rates of taxation for a defined period, etc.) for any organization that is the first to share knowledge of a new cyber threat or vulnerability with the Government and Australia's business community. Extra incentives could be provided for the first organization to provide a prevention, mitigation or remediation strategy that addresses that new cyber threat or vulnerability, if the Government wishes.

For industry, it can learn from the Government's approach to emergency situations, and streamline the ways in which it currently interacts with the public sector, so that in times of crisis, response is swift and smooth. This includes proactively ensuring that appropriate industry professionals meet the highest levels of demonstrated expertise in

information and cyber security and ideally possess the appropriate certifications and other qualifications that verify that.

22) To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

Whilst great progress has been made in increasing cyber awareness, it is ISACA's belief that progress is still needed. Lack of cyber awareness can and does drive poor choices by the consumer and increases the likelihood of the consumer to be taken in by scam activities. Likewise, if consumers are accepting of market offerings with sub-par cyber security, this does nothing to improve overall consumer choice or market offerings.

23) How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

In ISACA's considered opinion, an increased consumer focus on cyber security provides the one offering of most value to consumers: trust. However, as the Call for Views correctly notes, consumer cyber awareness is not a replacement for appropriately cyber secure products and services. As ISACA has noted in a number of responses to questions throughout this Call for Views, while consumers bear some responsibility for cyber security, the greater responsibility should lie with business that can ensure that cyber security is a core concern from conception, through development, and throughout the lifecycle of a product. Ultimately, ISACA believes, it is up to the consumer to play a prominent role in instigating change within the marketplace. To do so, however, requires increasing cyber awareness among consumers, providing appropriate venues for consumers to call attention to products that are less than cyber secure, and providing similarly appropriate mechanisms for industry and businesses to not only address those consumer concerns, but improve the cyber security of their products.

24) What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

In ISACA's considered opinion, citing specific examples of behavior-change campaigns or measures may not address this question adequately. ISACA believes that changes in behaviour, at scale, are the result of synergistic, unified efforts at the national level, such as the work done in Estonia over the past decade. Estonia's public and private sectors, as well as that nation's citizens, share an understanding that appropriate levels of cyber security are only achievable through mutual contribution, cooperation, and commitment. For Estonia, there is no 'one thing' that sets it apart; rather, great progress has been made by doing many things well, in concert with one another.

25) Would you like to see cyber security features prioritised in products and services?

When seat belts in vehicles first appeared in the marketplace, they were optional items; cars could easily be purchased without them. Today, that is no longer possible; seat belts are mandatory items in every car. Cyber security features and controls are no longer 'optional' considerations; they need to be perceived to be as necessary a part of a product or service as seat belts are a part of a modern-day automobile.

ISACA would like to see cyber security features prioritised in products and services from conception, through development, and along the length of the product lifecycle. In addition to prioritising features, however, there must be an even greater emphasis on the environment those features are created within.

Information and technology governance, leadership that possesses cyber security or governance expertise, a well-skilled, high-quality workforce of cyber security professionals possessing credentials attesting to their demonstrated ability—these are foundational elements the underpin the prioritisation of appropriate cyber security features in products and services. While having cyber security features prioritised in products in services is not only appropriate but welcome, creating an environment that 'builds in' such features as part of the normal course of business is, in ISACA's considered opinion, even more vital.

26) Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

Australia's 2020 Cyber Security Strategy will affect not only the nation, but those whom the Government would wish to work with as partners, and guard against as potential malicious actors. For this reason, ISACA believes that the Strategy would also benefit from an examination of best practices—as well as missteps—made by nations around the world. Their experience can be Australia's teacher, and the Government's cyber security endeavours in 2020 and beyond can be even more comprehensive, responsive and anticipatory for that input. As a complement to that, the Government could also look toward increasing its already strong presence on the international stage as a developer of internationally-developed and recognized cyber norms within regulatory, law enforcement, and other appropriate areas.

Consideration should also be given to the rapidly developing IT industry in Australia, and the need for the Government to provide the necessary structures to support its growth. Opportunities exist for the Government to provide this support in areas such as education, investment incentives, and information infrastructure (such as the National Broadband Network).