KordaMentha

2023-2030 Australian Cyber Security Strategy

Response to discussion paper

April 2023

kordamentha.com

Contents

Introduction

Responses to Discussion Paper

Appendix

Introduction to KordaMentha

Introduction

KordaMentha welcomes the opportunity to provide this submission on the Federal Government's consultation on the 2023-2030 Australian Cyber Security Strategy Discussion Paper.

KordaMentha is an independent and trusted firm providing specialist expertise across forensic accounting, restructuring, cyber security, financial crime, performance improvement and real estate services. Since 2002, our experts have been entrusted with some of the Asia-Pacific region's most complex and sensitive commercial situations. We work together to solve the challenges facing corporations, financiers, lawyers, private investors and government clients. Our team of almost 400 specialists extends across the Asia-Pacific and has experience ranging from cyber security, digital forensics, finance and real estate, law enforcement and the c-suite.

Through our extensive experience assisting our clients with their preventative cyber security challenges, KordaMentha's cyber advisory specialists work with boards, executives and organisations across the private and public sectors to evaluate their risk, develop mitigation strategies, implement solutions and help organisations when they experience an adverse cyber event. We assist organisations to manage their cyber risk effectively with the design and adoption of strong governance, operating models and risk reporting frameworks. Incorporating security compliance requirements into our approach also assists our clients to enhance their consumer and business partner confidence.

From a response, recovery and remediation perspective, clients also rely on KordaMentha cyber response experts to maintain business operations and minimise impacts following a cyber incident. Drawing on our broad range of incident response and digital forensic professionals, we assemble teams with the expertise tailored to each engagement. This allows us to provide a rapid, action-orientated and outcome-driven response at a time when inaction can be costly and lead to further loss. When required, we can adapt our approach from incident response to a detailed digital forensic investigation, potentially complemented by eDiscovery, financial impact quantification and expert witness assistance.

KordaMentha looks forward to the opportunity for continued collaboration with the Minister for Cyber Security as it progresses in the development of a robust and effective national cyber security strategy and look forward to ensuring a safer, more secure and more cyber resilient Australia.

Responses to Discussion Paper

Q1 – What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

KordaMentha forms the view that there are several areas the Federal Government should focus on to achieve the goal of making Australia the safest and most cyber secure nation in the world by 2030. These are broken down by sections below.

Building a shared national ambition related to cyber security

KordaMentha believes that raising the maturity of a nation's cyber security requires a concerted effort across government, industry, and community. Critically, it requires effective international collaboration with partners whose desire for cyber safe and secure societies parallel our own. This necessitates a strong alignment of ambition, intent and action, underpinned by the understanding that cyber security requires emphasis on culture change.

To foster such alignment, KordaMentha suggests clearly defining:

1. What the phrase "the most cyber secure nation in the world" means in a tangible and meaningful sense. More specifically, what it means to the nation, the public, business and academia – both across industries and to our communities. This definition should include a preamble explaining to everyday Australians as to why Australia should seek to become "the most cyber secure nation in the world" while transparently discussing the benefits and cost, both financially as well as socially, associated with delivering such an absolute ambition.
2. The methodology that will be used to measure and/or qualify the status of "the most cyber secure nation in the world".
3. The level of taxpayer-funded investment in cyber security to achieve this goal. KordaMentha posits that defining a yearly level of cyber security government expenditure expressed as a percentage of GDP is a meritorious approach that should be considered.
4. Which government department and/or agency will ultimately be responsible for attaining any goals that eventuate from the Strategy. KordaMentha notes that within the current Australian ecosystem, no single agency holds ultimate responsibility for cyber security matters, creating an accountability vacuum. While the re-establishment of a ministry dedicated to cyber security in 2022 was a welcome development,[1] the regulatory landscape for the cyber security sector in Australia is complex and poorly understood by individuals who are not entrenched and immersed in the cyber ecosystem.[2] As such, a clarification of who is responsible to take ownership and responsibility to ensure that Australia becomes "the most cyber secure nation in the world" is essential.
5. To what extent the Federal and State governments should collaborate to achieve any goals eventuating from the Strategy. KordaMentha notes that the fundamentals of cyber security do not differ at a local, state, national or even international level – yet it appears that there is little uniformity in the approach taken between state and federal governments in terms of standards adoption and cyber security skills frameworks, for example. KordaMentha recommends that state and federal governments should focus their collective efforts and resources on a unified approach to defining and achieving national resilience goals related to cyber security, rather than each government 'reinventing the wheel' so to speak.

Initiatives related to the *Privacy Act 1988*

KordaMentha supports the implementation of the 116 recommended proposals contained within the *Privacy Act Review Report* released by the Attorney-General's Department.[3] There is a prevailing view across the Australian economy that the current *Privacy Act 1988* (Cth) ('Privacy Act'), while well-intentioned, is both dated and not fit for purpose in its current form to meet the needs of the highly digital nature of the world we live in today. Implementing the proposed Privacy Act amendments will align Australia's privacy regime with those in the European Union, the UK, Canada,[4] Japan, Singapore and an increasing number of states in the United States of America. Such changes have the potential to represent the single biggest improvement in cyber security for Australia going forward, while increasing export and investment opportunities for Australian businesses abroad.

KordaMentha also supports strong and explicit statements by relevant regulatory bodies such as the Office of the Australian Information Commissioner ('OAIC') to ensure that legislative measures enlivened by Privacy Act amendments result in tangible and meaningful regulatory action. These statements should be followed by appropriate and timely action by the regulators to demonstrate that regulatory bodies can and will proactively administer their responsibilities and duties in matters where significant cyber security breaches have occurred. This should include willingness to employ punitive and pecuniary penalties where appropriate – measures which the OAIC has traditionally been reluctant to use.

Initiatives related to the *Corporations Act 2001*

KordaMentha notes that various regulatory authorities have suggested that responsibility for cyber security falls within the realm of directors' duties as contained in the *Corporations Act 2001* (Cth) ('Corporations Act').[5] These include obligations under care and diligence and good faith.[6] However, KordaMentha notes that ASIC has yet to prosecute a case against an officeholder based on a failure of a director meeting their governance duties because of a significant cyber security breach. While this may reflect broader criticism of ASIC's enforcement record,[7] KordaMentha notes that given the prevalence, scale and impact of cyber breaches, ASIC will need to be equipped and funded to ensure that complaints in relation to alleged breaches of directors' duties are promptly, diligently investigated and successfully prosecuted, where appropriate.

KordaMentha forms the view that the privacy of individuals represents a core element of corporate social responsibility ('CSR'). As such, KordaMentha considers that a data breach of private information can represent a violation of reasonable expectations of CSR, pursuant to circumstances related to that breach – namely the extent of preventative, detective and corrective risk management in place and the nature of the breach. However, KordaMentha notes that under the *Corporations Act 2001*, no current obligations exist for directors to have regard for the interests of stakeholders other than shareholders.[8] KordaMentha posits that in line with broader CSR initiatives relating to environmental and social goals (such as equal gender representation in senior management roles), directors' duties under the Corporations Act could be reviewed to incorporate some level of CSR stakeholder responsibility that incorporates a duty to the privacy of individuals.

Initiatives related to the security of critical infrastructure

KordaMentha notes the existence of the Security of *Critical Infrastructure Act 2018* (Cth) ('SOCI Act').[9] This act places obligations on entities deemed to operate in areas of critical infrastructure, and KordaMentha forms the view that the objects of the SOCI Act are essential, appropriate, and well-intentioned to strengthen cyber resilience across critical infrastructure sectors.[10]

In assisting clients with their SOCI Act obligations, KordaMentha notes that there is considerable ambiguity in relation to what provisions of the Act may be applicable to specific entities named within sectors that are nominally described to be critical infrastructure sectors of the economy. This issue is compounded with a lack of responsiveness to any enquires made to the Cyber and Infrastructure Security Centre ('CISC') for the purposes of clarifying responsibilities for entities seeking to manage their cyber security risk in accordance with SOCI Act requirements.

KordaMentha forms the view that a review of the performance of the SOCI Act pursuant to its objectives should be considered. The review should seek to:

1. Understand how entities operating within the critical infrastructure sector are enhancing their cyber security resilience in accordance with the statutory requirements under the SOCI Act.
2. Consider whether the SOCI Act in its current form helps entities meet new and emerging cyber security threat and attack vectors.
3. Determine the relative success of the SOCI Act, particularly in the context of the mega breaches at Optus, Medibank and Latitude Financial, entities which would have ostensibly fallen under SOCI Act obligations.

Initiatives related to the professionalisation of the Australian cyber security workforce

KordaMentha notes that no current guidance exists for Australian organisations relating to how they can accurately evaluate the competency of an individual who professes to be a professional within the cyber security sector. This is despite requirements articulated within regulations such as APRA CPS-234, for example, that 'An APRA-regulated entity must ensure that testing is conducted by appropriately skilled and functionally independent specialists'[11] and that 'information security control assurance is provided by personnel appropriately skilled in providing such assurance'.[12]

Given the access that cyber security practitioners have to sensitive information, KordaMentha believes that a compelling need exists for the professionalisation of the Australian cyber security workforce. Further, such a professionalisation scheme should be approved, endorsed and promoted by Government at a Federal, State and Local level. The manner and form of a proposed professionalisation scheme is discussed in detail at Questions 11 and 12 of this submission.

Q2 – What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

KordaMentha forms the view that the main legislative instruments that should be considered for review and reform by Government to enhance the cyber resilience of the digital economy include:

- The *Privacy Act 1988*, noting there is work already underway in relation to reform of the Privacy Act.
- The *Corporations Act 2001*.
- The *Security of Critical Infrastructure Act 2018*.

For a detailed set of recommendations related to these legislative instruments, please refer to Question 1 of this submission.

Question 2(a). What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

KordaMentha forms the view that mechanisms to improve cyber security standards across the Australian economy need to combine a range of incentives to encourage behaviours and practices that enhance and boost cyber security resilience, coupled with appropriate enforcement and/or punitive measures to ensure that organisations undertake the appropriate levels of commitment to protect their information assets.

KordaMentha posits that incentives could include tax concessions or offsets for businesses that invest in cyber security resilience, particularly those focused on the people and process elements of cyber security. As an example, such investments could include:

- Incentives such as tax concessions or subsidies to undertake independent cyber security maturity assessments conducted by accredited cyber security professionals against the ASD Essential Eight Maturity Model,[13] the NIST Cyber Security Framework,[14] ISO/IEC 27001[15] and/or ISO/IEC 27701.[16]
- Incentives such as time-limited tax concessions or subsidies to assist in the hiring of cyber security professionals by a yet-to-be-determined Australian cyber security professionalisation scheme by organisations.
- Tax concessions to incentivise the training and accrediting employees for the purposes of cyber security resilience by the organisation.
- Incentives such as subsidies or tax concessions to undertake formal accreditation to ISO/IEC 27001 or ISO/IEC 27701 compliance.

While KordaMentha is of the firm view that an approach based on incentives will yield optimum long-term results, KordaMentha recommends that a stronger enforcement regime should exist in instances where a cyber security breach could have been avoided if not for the existence of reasonably simple and straightforward cyber security risk management processes. KordaMentha notes that very limited punitive regulatory activity has occurred to date based on cyber breach, and the perception does exist in some quarters that regulators such as the OAIC and ASIC are reluctant to dispense with punitive actions. Undoubtedly, this fact likely contributes to a sense of apathy by some organisations who might conclude that regulators will not investigate and/or act against them in the event of a cyber breach.

Question 2(b). Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

KordaMentha believes that a wide-ranging review of the SOCI Act should be considered. The review should seek to:

1. Understand how entities operating within the critical infrastructure sector are enhancing their cyber security resilience in accordance with the statutory requirements under the SOCI Act.
2. Consider whether the SOCI Act in its current form helps entities meet new and emerging cyber security threat and attack vectors.
3. Determine the relative success of the SOCI Act, particularly in the context of the mega breaches at Optus, Medibank and Latitude Financial, entities which would have ostensibly fallen under SOCI Act obligations.

Please refer to Question 1 of this submission for ancillary information.

Question 2(c). Should the obligations of company directors specifically address cyber security risks and consequences?

KordaMentha notes that various regulatory authorities have suggested that responsibility for cyber security falls within the realm of directors' duties as contained in the *Corporations Act*.[17] These include obligations under due care, due diligence and good faith.[18] KordaMentha supports the view that the obligations of officeholders should include those related to cyber security, specifically cyber security risk management.

KordaMentha supports the requirement that corporate officeholders, including company directors, demonstrate a level of knowledge of cyber security commensurate with the organisational risk that cyber security presents in the digital era. And given that information related risks have been demonstrated to hold the same level of importance in terms of potential impact as financial risk, human risk and other major organisational risks, KordaMentha posits that information security requires a similar level of scrutiny and controls at a board level. KordaMentha does not contend that all corporate officeholders, including company directors, should be or should be required to become fully accredited cybersecurity professionals. However, KordaMentha does contend that proposals discussed in the United States, namely, that boards describe the level of cyber security expertise that exists at a board level of an organisation,[19] could represent a possible step forward for the Australian context.

In addition, KordaMentha forms the view that the privacy of individuals represents a core element of CSR. As such, KordaMentha considers that a data breach of private information can represent a violation of reasonable expectations of CSR, pursuant to circumstances related to that breach – namely the extent of preventative, detective and corrective risk management in place and the nature of the breach. However, KordaMentha notes that under the *Corporations Act 2001*, no current obligations exist for directors to have regard for the interests of stakeholders other than shareholders.[20] KordaMentha posits that in line with broader CSR initiatives relating to environmental and social goals (such as equal gender representation in senior management roles), directors' duties under the *Corporations Act* could be reviewed to incorporate some level of CSR stakeholder responsibility that incorporates a duty to the privacy of individuals.

Question 2(d). Should Australia consider a Cyber Security Act, and what should this include?

KordaMentha contends that information security, including electronic security popularly referred to as 'cyber security', should form part of an amended Privacy Act as described at Question 1 of this submission. KordaMentha does not believe that there is a need for a separate act aimed purely at cyber security considerations, given that cyber security represents a subset of information security, which in turn is driven by privacy requirements.

Should recommendations made at Question 1 in relation to an updated Privacy Act be adopted which will see the Act fit for current and future needs, KordaMentha believes that a sensible approach would be to develop delegated legislation and regulation for the Privacy Act that enliven obligations relating to cyber-specific considerations and which can be updated easier and more frequently as circumstances, technology and the market changes.

Question 2(e). How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cybersecurity, and are there opportunities to streamline existing regulatory frameworks?

KordaMentha posits that consultations through means such as online surveys, phone calls and polling to select business stakeholders to gather constructive feedback and capture the sentiment on the matter involved would be appropriate to monitor the regulatory burden of cyber security obligations on Australian businesses.

> "KordaMentha believes that there are opportunities to streamline regulatory frameworks..."

KordaMentha believes that there are opportunities to streamline regulatory frameworks, such as areas of overlap between the OAIC, AUSTRAC, the ACCC and ACMA, for example. However, as indicated at Question 1 of this submission, KordaMentha notes that within the current Australian ecosystem, no single agency holds ultimate responsibility for cyber security matters, creating an accountability vacuum. This is of concern given the regulatory landscape for cyber security in Australia is complex and poorly understood by individuals who are not entrenched and immersed in the cyber ecosystem.[21] KordaMentha reiterates that clarification of who is responsible to take ownership and responsibility of matters related to cyber security will assist in simplifying the cyber ecosystem, ensuring a single point of accountability for all matters related to cyber security and ultimately will assist with easing regulatory burdens.

Question 2(f). Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?

KordaMentha does not believe that a general prohibition of ransoms or extortions demanded by cyber criminals by victims and/or insurers should be considered. KordaMentha does note that this subject is both complicated and controversial, noting a myriad of ethical and moral considerations at play when considering ransom and/or extortion payments, and posits that no simple answer exists to the question.

KordaMentha forms the view that the preferable position in relation to ransom or extortion payments should always be to not pay a ransom or extortion demand. KordaMentha understands that, notwithstanding any AML/CTF considerations inherent in any payment to anonymous cyber criminals, any ransom and/or extortion payment will further embolden and incentivise cyber criminals in performing subsequent acts of a similar nature.

KordaMentha strongly believes that should organisations implement appropriate preventative cyber risk management strategies, it would be rare for organisations to need to pay a ransom or extortion demand as the risk of a cyber breach is significantly minimised. It is for this reason that a primary focus of the cyber security services that KordaMentha offers to clients rests in the preventative advisory phase of the cyber security lifecycle.

KordaMentha notes that in some very limited circumstances, organisations and individuals may feel compelled, either financially or on a point of ethics, to consider payment of a ransom or extortion demand. For example, if human life and/or safety is at risk and there is no reasonable workaround to the issue, then a compelling reason to make a ransom or extortion payment may exist. This scenario becomes problematic should a general prohibition on ransom and/or extortion payments exist in statute.

Question 2(g). Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

KordaMentha believes that the Federal Government should clarify its position in relation to the payment or non-payment of ransoms of companies. Please refer to the response at Question 2(f) of this submission.

> …if an organisation were to consider paying a ransom, it should be obligated to inform law enforcement that it intends to make a payment.

KordaMentha believes that if an organisation were to consider paying a ransom, it should be obligated to inform law enforcement that it intends to make a payment. It should also be required to obtain specialist and accredited legal and technical incident response advice in relation to the matter to ensure it has undertaken all necessary steps and measures to avoid the payment of a ransom.

Q3 – How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

KordaMentha believes that an international approach to cyber risk management will be necessary to adopt long-term to mitigate cyber risk, build cyber resilience and better respond to cyber security incidents.

KordaMentha believes that multilateral treaty approaches, such as the *Budapest Convention*,[22] agreed to by nation states connected to the Internet, could form a key component of better cyber resilience at an international level. KordaMentha notes that while Australia is a party to the Convention, nation states including regional neighbours as well as nation states that are often cited as sources of cyber attacks are not. As such, KordaMentha contends that international diplomacy should continue efforts to ensure that all nation states become party to the Convention. KordaMentha also contends that given the criticality of cyber security in the modern and globalised hyper-digital world we all live in, trade negotiations with other nation states should consider a pre-requisite that that nation state is a party to the Convention.

> …efforts should be undertaken for Australia to seek adequacy with the European Union.

KordaMentha holds the view that once the Privacy Act has been amended (as described at Question 1 of this submission), efforts should be undertaken for Australia to seek adequacy with the European Union ('EU') GDPR,[23] a legislative framework which is now considered to be the 'de-facto' standard in relation to privacy and one that is considered to be a primary source of insight and inspiration by an increasing number of nation states. This will ensure that Australia can remain at the forefront of inflowing investment opportunities, while providing export opportunities through Australian organisations opportunities to maximise the provision of services to overseas consumers and businesses.

Q4 – What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective.

KordaMentha forms the view that Australia's international cyber security partnerships should be based on multilateral approaches such as the *Budapest Convention*. Please refer to Question 3 of this submission.

Q5 – How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space.

KordaMentha forms the view that Australia's international cyber security work, including standards-setting processes, should be based on multilateral approaches such as the *Budapest Convention*, as described at Question 3 of this submission.

KordaMentha also believes that Australia's continuing participation by Standards Australia in the International Standards Organisation ('ISO') is crucial to ensure that Australian insights, expertise and experience can continue to contribute to international standards related to cyber security.

Q6 – How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities.

KordaMentha strongly believes that annual and independent cyber security maturity assessments and audits of the Commonwealth Government departments should be undertaken by accredited and security cleared external providers.

KordaMentha notes that the Australian National Audit Office ('ANAO') 'Cyber Security Strategies of Non-Corporate Commonwealth Entities' report published in March 2021 illustrated that cyber risk mitigation strategies undertaken by Government departments were 'not fully effective',[24] with only 24% of Commonwealth entities being compliant with mandatory Top Four mitigation strategies and 72% of entities not implementing PSPF Policy 10 (Management of Cyber Security Supply Chain Risks).[25] Similar results have ensued at a state level in NSW[26] and Victoria.[27]

> "... ensuring that Government departments are practicing good cyber security offers strong leadership to other sectors of the Australian economy."

Given that Government is an exemplar of strong risk management practices, KordaMentha contends Government plays an essential role in demonstrating to the private sector and Australian society more broadly why strong cyber risk management is essential. As such, ensuring that Government departments are practicing good cyber security offers strong leadership to other sectors of the Australian economy.

Q8 – During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ ACSC without the concern that this will be shared with regulators?

KordaMentha believes that for organisations to obtain support from the ASD and ACSC, this support should not come with any confidentiality concerns, including between Government departments and regulators. KordaMentha believes that if this were to be at question, there would be reluctance to seek support from Government and, thus, could ultimately prove to be highly counter-productive for cyber resilience. As such, KordaMentha recommends that an explicit obligation of confidentiality should exist upon the ASD and the ACSC in relation to the potential sharing of incident information with regulators.

Q9 – Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

KordaMentha believes that expansion of the existing data breach notification regime to reporting of ransomware and/or extortion demands should be considered. This response is articulated in detail at Question 2(g) of this submission.

Q11 – Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

KordaMentha notes that the Australian context for cyber threats is no different to any other nation state. As such, while there may be an element of tailoring required, primarily in relation to defence localisation requirements, any tailoring of cyber skills uplift should be limited to these remits only. It must be noted that KordaMentha is a strong believer, support and advocate for standards-based approaches in cyber security. It is for this reason, for example, that KordaMentha has embarked on and has successfully achieved ISO/IEC 27001 accreditation,[28] and actively supports Australian organisations to achieve maturity towards standards such as ISO/ISC 27001 for information security and ISO/IEC 27701 for privacy.

In relation to professionalisation of the cyber security sector, KordaMentha forms the view that some level of professionalisation is required, given the criticality of work undertaken by cyber security professionals and the level of access to sensitive information that cyber security professionals inherently have through their day-to-day work. KordaMentha notes and supports the AustCyber Australian Cyber Security Professionalisation Program ('ACSP') for which Tony Vizza, Executive Director at KordaMentha, is a member of the co-design team.[29] Related to this, KordaMentha forms the view that while role definitions within cyber security could be tailored for local needs to some extent, any cyber skills and recognition of cyber skills should be aligned and/or mapped to international cyber skills frameworks such as NICE,[30] SFIA,[31] and CIISec.[32] This will help facilitate the entry of overseas cyber security professionals seeking to move to Australia for work.

> "KordaMentha strongly supports the notion that any professionalisation scheme should be aligned to ISO/IEC 17024 and/or approved by the Federal Government Professional Standards Council."

Consistent with the response provided at Question 12 and our support for standards-based approaches for cyber security, KordaMentha strongly supports the notion that any professionalisation scheme should be aligned to ISO/IEC 17024[33] and/or approved by the Federal Government Professional Standards Council.[34] This will ensure that the Government's STEM agenda, incorporating cyber skills, will be driven by industry needs that include Government and private sector needs, recognised by ISO/IEC 17024 and by the Professional Standards Council.

Q12 – What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

KordaMentha believes that there is a critical need for Government to support Australia's cyber security workforce, particularly in creating policy that supports a well-educated, competent and experienced workforce. KordaMentha notes that numerous studies from entities such as AustCyber locally and (ISC)^2 at a global level illustrate the significant cyber skills gap that exists here in Australia and across the world. AustCyber predicts that there will be a shortage of 3,000 cyber security workers by 2026,[35] while (ISC)^2 claims that there is a shortage of 39,496 workers who perform at least 25% of their work in cyber security in Australia today.[36] KordaMentha also notes that there are over 5,400 roles advertised in Australia as of April 2023 recruiting for individuals who are CISSP certified[37] and over 12,000 roles being advertised across Australia with the term 'cyber security' included in the role description.

KordaMentha forms the view that some level of professionalisation is required for the cyber security sector, given the criticality of work undertaken by cyber security professionals and the level of access to sensitive information that cyber security professionals inherently have through their day-to-day work. As indicated at Question 11, KordaMentha notes and supports the AustCyber Australian Cyber Security Professionalisation Program (ACSP) for which Tony Vizza, Executive Director at KordaMentha, is a member of the co-design team.[38]

KordaMentha considers that any professionalisation scheme should be aligned to international industry standards. This will ensure that any scheme implemented for the Australian market can easily be understood by migrants entering Australia for work.

KordaMentha believes that the ISO/IEC 17024 standard, governing personnel accreditation bodies, represents the ideal standard to adopt for an Australian professionalisation scheme for cyber security. KordaMentha further notes that all well-respected international cybersecurity certifications in the world today which denote knowledge, skills, experience, competency and adherence to a code of ethics, are ISO/IEC 17024 accredited. These include industry accreditations issued by not-for-profit industry bodies such as the (ISC)^2 CISSP, CCSP, CSSLP and SSCP, the ISACA CISM, CISA, CRISC and CGEIT, the PECB ISO27001 Auditor/Implementer series of certifications and the IAPP CIPP/E, CIPP/US, CIPM and CIPT, to name a few.[40]

KordaMentha also considers that as part of an improvement of Australia's cyber security workforce capability competency, a focus on diversity is essential to ensure that the field attracts individuals with diverse backgrounds, experiences, skills and methodologies. To this effect, KordaMentha supports the work of organisations such as the Australian Women in Security Network (AWSN)[41] who focus on ensuring there is an appropriate gender balance within cyber security.

In relation to a potential accreditation scheme for the cyber security sector, KordaMentha notes and endorses work undertaken by Tony Vizza, Executive Director at KordaMentha in a personal capacity, in association with Prof. Jill Slay AM from the University of South Australia. This work, a whitepaper for the professionalisation of the Australian cyber security workforce titled 'A Scheme for the Professional Recognition of Australian Cyber Security Professionals', is contained in the Appendix.

Q16 – What opportunities are available for Government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

KordaMentha forms the view that the Federal and State Governments should make domestic capability a priority for the cyber security industry. This will result in a greater proportion of the Retained Economic Benefit (REB) pertaining to cyber security products and services remaining under domestic control. KordaMentha notes that cyber security market sector growth, greater market opportunities for Australian cyber security businesses and the capacity to establish export capability in cyber security represent areas of strategic significance for Government.

KordaMentha notes that despite an increase in security companies in Australia (350 entities in 2020, as noted by AustCyber), 88% of that number have fewer than 100 employees. Given that most of these organisations are very small, often competing with other another for similar work, there is a perception that a lack of a genuine and viable domestic ecosystem exists. Additionally, sentiment does exist in the notion that Australian cyber security companies often experience greater traction in overseas markets than they do locally.

> "KordaMentha believes that Government must prioritise a viable and thriving nucleus of domestic capability in-country before export becomes a focus for Australian cyber security solutions providers."

Noting the intense international competitiveness that exists for truly innovative cyber security solutions, KordaMentha believes that Government must prioritise a viable and thriving nucleus of domestic capability in-country before export becomes a focus for Australian cyber security solutions providers. KordaMentha encourages the work undertaken by AustCyber in this regard, particularly in relation to AustCyber's Sector Competitiveness Plan.[41]

Q19 – How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

KordaMentha forms the view that there are two very distinct areas of emerging technology that will need to be considered in the short term to ensure that risks are managed in the long term. These two areas are Internet of Things (IoT) security as well as security in relation to Artificial Intelligence (AI).

Internet of Things security

In relation to IoT security, KordaMentha believes that industry organisation initiatives such as the IoT/OT Security Trust Mark Certification[42] and Cybersecurity Labelling Scheme (CLS) will ensure better IoT and Operational Technology (OT) security. The CLS is a leading innovative and unique international framework completely developed in Australia, setting clear benchmarks for existing and emerging technologies to harmonise and conform with globally and supports new technology privacy, safety and 'security by design' initiatives.

KordaMentha also notes and supports recent efforts from the ACSC, partnering with the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), National Cyber Security Centre (NCSC) in the UK, Canadian Centre for Cyber Security (CCCS) and international partners in Germany, the Netherlands and New Zealand urging manufacturers of IT products and services, including IoT security, to 'revamp their design and development programs to permit only Secure-by-Design and Default products to be shipped to customers'.

Finally, KordaMentha notes efforts in other jurisdictions around the world seeking to improve IoT security. For example, the state of California in the U.S. legislates a minimum level of protection for consumers in IoT products.[43] KordaMentha posits that there may be merit in Australia considering regulation that mandates minimum security requirements for IoT security in consumer devices.

Artificial Intelligence

KordaMentha appreciates the inherent potential that exists with AI and its potential contributions to increasing productivity and efficiency, not just in cyber security but across large sectors of the economy. However, KordaMentha forms the view that some level of regulation in relation to the use and proliferation of AI needs to be considered by Government, particularly given its documented use by cyber threat actors to perform acts of cybercrime.[44] KordaMentha notes efforts in the European Union to regulate artificial intelligence systems[45] and believes that a similar approach in Australia may be justified and should be considered expeditiously given the rapid developments in this space.

Q20 – How should Government measure its impact in uplifting national cyber resilience?

KordaMentha forms the view that Government should measure its impact in uplifting national cyber resilience in using defined metrics on cybercrime and breach statistics that are updated at least quarterly. KordaMentha notes that the OAIC publishes information bi-annually while the ACSC publishes a report annually. While KordaMentha notes that these reports provide useful information, follow-up data related to incidents reported in the OAIC and ACSC reports are non-existent.

KordaMentha believes potentially valuable data points exist in relation to follow-up data at the back of an NDB notification – for example, in reporting anonymised statistics of breach size in terms of financial harm, reputation/goodwill loss, whether a cyber insurance policy existed and was claimed upon and other data points that can reinforce for Australian organisations the harm that cyber security breaches can result in.

Key contributing authors

Brendan Read
Partner
Brisbane

Peter Chapman
Partner
Sydney

Rahul Lobo
Partner
Melbourne

Tony Vizza
Executive Director
Sydney

Guillaume Noé
Executive Director
Brisbane

End notes

1. I. Bongiovanni, “Australia finally has a dedicated minister for cyber security. Here’s why her job is so important,” The Conversation, Jun. 03, 2022. http://theconversation.com/australia-finally-has-a-dedicated-minister-for-cyber-security-heres-why-her-job-is-so-important-184322.
2. Patrick Fair, “Australian Cyber Security and Online Safety Infrastructure Chart.” Technology Law Pty Ltd, Jul. 2020. [Online]. Available: https://www.patrickfair.com/_files/ugd/ce391e_546b5b105fe64af79037d0d2fe70d329.pdf.
3. Attorney-Generals Department, Australian Government, “Privacy Act Review Report 2022,” Feb. 2022 pages 5-16.
4. IAPP, “Global Comprehensive Privacy Law Mapping Chart,” Apr. 2022. https://iapp.org/resources/article/global-comprehensive-privacy-law-mapping-chart/ (accessed Apr. 21, 2023).
5. ASIC, ‘Chair’s Remarks at the AICD Australian Governance Summit 2023’, (speech, 2 March 2023) <https://asic.gov.au/about-asic/news-centre/speeches/chair-s-remarks-at-the-aicd-australian-governance-summit-2023/>.
6. Corporations Act 2001 (Cth) (‘Corporations Act’) s 180-1.
7. Patrick Durkin, ‘ASIC’s Enforcement “Completely Unacceptable”’, Australian Financial Review (19 March 2023) <https://www.afr.com/policy/economy/asic-s-enforcement-record-completely-unacceptable-20230319-p5cte3>.
8. Paul Redmond, Corporations and Financial Markets Law, 7th Ed, 2017. [2.208] 80.
9. Security of Critical Infrastructure Act 2018 (Cth) (‘SOCI Act’).
10. Ibid s 3.
11. Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 1 of 2018 (Prudential Standard CPS 234 Information Security) (Cth) s 30.
12. Ibid s 33.
13. Australian Signals Directorate / Australian Cyber Security Centre, “Essential Eight Maturity Model” (November 2022) <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model>.
14. National Institute for Standards and Technology (NIST), “Framework for Improving Critical Infrastructure Cybersecurity – Version 1.1” (April 2018) <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
15. ‘ISO/IEC 27001:2022 – Information Security Management Systems’, International Standards Organisation (ISO) <https://www.iso.org/standard/27001>.
16. ‘ISO/IEC 27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines’, International Standards Organisation (ISO) <https://www.iso.org/standard/71670.html>.
17. ASIC, ‘Chair’s Remarks at the AICD Australian Governance Summit 2023’, (speech, 2 March 2023) <https://asic.gov.au/about-asic/news-centre/speeches/chair-s-remarks-at-the-aicd-australian-governance-summit-2023/>.
18. Corporations Act 2001 (Cth) (‘Corporations Act’) s 180-1.
19. Pearlson, Dr Keri and Chris Hetner, ‘Is Your Board Prepared for New Cybersecurity Regulations?’ (11 November 2022) Harvard Business Review <https://hbr.org/2022/11/is-your-board-prepared-for-new-cybersecurity-regulations>.
20. Paul Redmond, Corporations and Financial Markets Law, 7th Ed, 2017. [2.208] 80.
21. Patrick Fair, “Australian Cyber Security and Online Safety Infrastructure Chart.” Technology Law Pty Ltd, Jul. 2020. [Online]. Available: https://www.patrickfair.com/_files/ugd/ce391e_546b5b105fe64af79037d0d2fe70d329.pdf.
22. Council of Europe, Convention on Cybercrime, 23 November 2001 < https://www.coe.int/en/web/cybercrime/the-budapest-convention>.
23. European Commission, ‘Adequacy Decisions’ <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>.
24. Australian National Audit Office, ‘Cyber Security Strategies of Non-Corporate Commonwealth Entities’, (19 March 2021) <https://www.anao.gov.au/sites/default/files/Auditor-General_Report_2020-21_32.pdf> 9.
25. Ibid 6.
26. ‘Detecting and Responding to Cyber Security Incidents’, Audit Office of New South Wales (2 March 2018) <https://www.audit.nsw.gov.au/our-work/reports/detecting-and-responding-to-cyber-security-incidents->.
27. ‘Vic Audit Warns of Weak IT Controls in Council Systems’, iTnews 27 February 2023. <https://www.itnews.com.au/news/vic-audit-warns-of-weak-it-controls-in-council-systems-591346>.
28. ‘KordaMentha Achieves Firm-Wide ISO 27001 Certification’, KordaMentha <https://kordamentha.com/insights/firm-wide-ISO-27001-Certification>.
29. AustCyber, ‘Australian Cyber Security Professionalisation Program’,<https://www.austcyber.com/acsp>.
30. National Initiative for Cybersecurity Education (NICE), U.S. Department of Commerce, United States Government, ‘NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework’, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>.
31. ‘The Global Skills and Competency Framework for a Digital World’, SFIA <https://sfia-online.org/en>.
32. ‘CIISec | The Home of Cyber’, CIISec <https://www.ciisec.org/CIISEC/CIISEC/Home.aspx>.
33. International Standards Organisation (ISO), ‘ISO/IEC 17024:2012 Conformity Assessment – General Requirements for bodies operating certification of persons’, https://www.iso.org/standard/52993.html.
34. Professional Standards Council, <https://psc.gov.au/>.
35. AustCyber, ‘SCP-2022 - Homepage | AustCyber’, <https://www.austcyber.com/resources/sector-competitiveness-plan>.
36. (ISC)2, Cybersecurity Workforce Study 2022, <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx> 8.
37. LinkedIn, <www.Linkedin.com>. CISSP keyword search under open jobs
38. AustCyber, ‘Australian Cyber Security Professionalisation Program’ <https://www.austcyber.com/acsp>.
39. ANSI National Accreditation Board, ‘ISO/IEC 17024 Personnel Certification Bodies – Accreditation Directory’, < https://anabpd.ansi.org/Accreditation/credentialing/personnel-certification/ALLdirectoryListing?menuID=2&prgID=201&statusID=4>.
40. Australian Women in Security Network (AWSN) <https://www.awsn.org.au/>.
41. AustCyber, ‘SCP-2022 - Homepage | AustCyber’, <https://www.austcyber.com/resources/sector-competitiveness-plan>.
42. IoT Security Trust Mark <https://iotsecuritytrustmark.org/>.
43. Senate Bill No. 327 Information Privacy: Connected Devices (California), <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327>.
44. Ravichandran, Hari, ‘Council Post: How AI Is Disrupting And Transforming The Cybersecurity Landscape’, Forbes <https://www.forbes.com/sites/forbestechcouncil/2023/03/15/how-ai-is-disrupting-and-transforming-the-cybersecurity-landscape/>.
45. ‘The EU’s Artificial Intelligence Act, Explained’, World Economic Forum (28 March 2023) <https://www.weforum.org/agenda/2023/03/the-european-union-s-ai-act-explained/>.

Appendix

A SCHEME FOR THE PROFESSIONAL RECOGNITION OF AUSTRALIAN CYBER SECURITY PROFESSIONALS

TONY VIZZA & JILL SLAY
[redacted]

INTRODUCTION

How Government, Industry and Academia can Professionalise the Cyber Security Profession in Australia

This paper offers evidence-based and internationally proven guidance to Australian Government, Industry and Academia stakeholders in relation to setting up a professional accreditation scheme for the cyber security workforce in Australia.

This guidance is based on the adoption of mechanisms that are well understood and valued by the market and industry, coupled with flexibility that caters to individuals who may follow non-traditional pathways to entry into the cyber security profession.

The mechanisms described in this scheme are aligned with internationally recognised standards, congruent with similar schemes that have been adopted by some of Australia's international partners, which incorporate respected indicators of competency and success. Most importantly, the guidance will rely on collaboration and partnerships within the existing value chain to ensure scalability and maximum penetration of the scheme across the Australian cyber security ecosystem.

ANALYSIS OF THE ISSUES WITHIN THE AUSTRALIAN CYBER SECURITY PROFESSION TODAY

There is broad consensus across many sectors of the Australian economy, including government, industry, and academia, that the cyber security sector requires some levels of professionalisation to bring it in line with standards of competence that are commonly in existence in more established industries. By introducing standards of competency for individuals working within the sector which utilises and aligns to many of the credentials and qualifications that already exist for cyber security professionals, professional work experience and background checks, such a scheme would help in answering long-standing questions which have often plagued and compounded efforts to address the cyber skills shortage. These include:

- Who, or what, is a 'cyber security professional'. Robust discussions often centre on whether experienced information technology professionals can, or should, be considered a cyber security professional; or what percentage of a technology professionals day-to-day work needs to take place in specialties related to cyber security for that person to be considered a cyber professional; or how much 'industry experience' a cyber security professional should have; or even what does 'industry experience' entail.
- Which professional standards body oversees the cybersecurity profession and manages professional development, oversees matters of professional ethics and promulgates professional standards. Previous work with the previous federal Liberal National government allowed the development of the Australian Computer Society (ACS) 'Certified Professional' (Cyber) and 'Certified Technician' (Cyber) designations, developed in conjunction with (ISC)^2 and ISACA, back in 2017. However, this professional standard that was established in cyber security has not been widely valued or accepted by the cyber security ecosystem, nor has it been policed in any way by the Federal Government or been well-promoted by the ACS.
- The lack of a formal education and career pathway for aspiring cyber security professionals to follow. Different stakeholders within the cyber security ecosystem such as universities, TAFE's, private colleges, certification bodies and other training providers such as technology vendors extoll the perceived value of their own offerings, often understating the importance of other offerings which are portrayed as competing. While it is true that each stakeholder can bring value to the ecosystem, there can be confusion, mischaracterisation, or a misunderstanding as to what the value of a specific offering may represent, both to interested individuals as well as more generally to the market. An oft-stated view that is raised by industry is that recently graduated individuals are not 'job ready', for example. Similarly, the claim that tertiary education courses do not reflect the needs of industry is also frequently heard.

- The focus on bringing computer science graduates from developing countries and allowing them to study cyber security without any guarantee they will be clearable even when they have permanent residency or citizenship. This unfortunate circumstance exists with many international graduates (particularly those who hold a Master of Cyber Security) who have a keen desire to remain in Australia and gain permanent residency and citizenship. However, they are effectively unemployable primarily due to the requirement for baseline and higher clearances across Federal and State government systems, in banking and finance, the telecommunications sector and many critical infrastructure sectors where large numbers of vacancies currently exist. As a result, these graduates often take menial employment in jobs that are wholly unrelated to their education, failing to join the cyber security sector entirely and compounding the skills gap even further.
- The confusion for the Australian tertiary education system about accreditation of cyber security degrees, particularly master's degrees, by the ACS as 'Computer Science' degrees. This issue remains unresolved. It means that to encourage international students to take up these studies in Australia for the purposes of potentially attaining permanent resident status, the sector is creating degrees ostensibly called 'cyber security' degrees which incorporate the overly technical elements of traditional computer science degrees, elements that serve no practical purpose in an employment context. As a result, these degrees in their current design do not equip the student for the Australian cyber security market once they have graduated.
- The shortage of Australian tertiary researchers and teachers with real-world Australian industry work experience, and as a result, shortage of industry certified and/or accredited individuals in cyber security that can demonstrate that work experience. There has been very little interest from Australian domestic students in taking up PhD studies in cyber security. This has subsequently resulted in a lack of Australian domestic professionals remaining in the tertiary education sector, since there is a significant salary disparity between what is offered in industry and government. This has resulted in the current (and younger) generation of postdoctoral and lecturing professionals having come largely from developing countries after exiting their PhDs with a very narrow and theoretical understanding of cyber security. While these academic achievements assure significant, such individuals arguably have a singular ability to publish papers and remain in Australia to gain permanent residency. Often, these individuals have no industry-based work experience in their country of origin or in Australia. As a result, graduates who are taught by these academically gifted but inexperienced professionals are often unfit for the needs of the Australian workforce.
- The rapid pace of change that inherently exists in cyber security, and more broadly in the IT sector. Often education programs in cyber security can be out of date by the time they can be operationalised. Delivering an up-to-date education program that incorporates a relevant and up to date curriculum is daunting and the rapid change that happens in the sector further hinders the crystallisation of an accepted education and career journey for cyber security professionals.
- A lack of enough job-experienced people with demonstrable competence in cyber security, coupled with long-standing issues related to the relatively homogenous nature of the existing workforce and inclusivity of minority and neurodiverse individuals. The cyber skills gap and workforce shortage both Australia and more broadly, around the world, is well documented. However, it goes beyond just the insatiable demand for cyber (and IT) professionals. Despite initiatives to diversify the IT profession and promote the sector to women, women still only make up 28% of the ICT workforce in Australia[1] and only 18.3% of the cyber security workforce[2]. Similarly, only 128 individuals from ATSI backgrounds work within information security today.[3] This reflects the general trend within STEM (science, technology, engineering, and mathematics), with female participation in STEM education remaining at not too dissimilar levels over the last 20 years, despite the focus on increasing female participation in STEM.[4]

[1] ACS, *Australia's Digital Pulse – Driving Australia's International ICT Competitiveness and Growth, 2018,* https://www.acs.org.au/content/dam/acs/acs-publications/aadp2018.pdf.

[2] AISA, *Australian Cyber Security Skills and Jobs Study, 2020*, https://aisa.org.au/common/Uploaded%20files/Research/AISA_NSW%20Report_2020_Final.pdf

[3] ASPI, *Too Few Indigenous People in Tech, 2021,* https://ia.acs.org.au/article/2021/too-few-indigenous-people-in-tech.html.

[4] DISR, *Second National Data Report on Girls and Women in STEM, 2021,* https://www.industry.gov.au/news/second-national-data-report-on-girls-and-women-in-stem.

CRITICAL SUCCESS FACTORS FOR A COMPELLING, INDUSTRY SUPPORTED PROFESSIONALISATION SCHEME

In seeking to establish a successful professionalisation scheme, Government, Industry and Academia will need to consider the current Australian and international cyber security ecosystem as it currently stands. It will be critical for the any future scheme to incorporate the best, most recognised, and most valuable attributes of the existing ecosystem and use those attributes to advance and accelerate progression to the desired end state – which is to establish a scheme where the Australian cyber security workforce is better skilled, experienced, and competent to handle current, new, and emerging cyber threats.

In this paper, it is contended that a professionalisation scheme needs to be founded and guided by the following core principles:

1. The scheme needs to be delivered at minimal cost to individuals.
2. The scheme needs to develop strong support in the tertiary sector given its own skills shortage, its lack of ability to develop fit-for-purpose cyber security offerings particularly given its dependency on ACS accreditation.
3. The scheme needs to develop employment pathways which are not hindered by lack of ability to gain an AGSVA or other clearance, even at baseline. This needs to cater for international students graduating from Australian cyber security pathways and those who are brought into the country as migrants skilled in cyber security. It should be noted that as it stands, the ACS is the gate keeper for both sets of these potential employees.
4. The scheme must not hinder or block emerging new entrants into the marketplace, regardless of their status as a school leaver or career changer.
5. The scheme must not create an additional set of certifications or accreditations, but rather, must leverage existing and respected market certifications and accreditations.
6. The scheme must incorporate methods that recognises professional competency in cyber security. This includes recognition of hands on, paid work experience, as well as educational background an individual has attained.
7. The scheme must embed a strong set of professional standards and a code of ethics that strengthens, protects, and promotes public faith in the sector.
8. The scheme should incorporate an element of verification of background, character and/or ethical standing.
9. The scheme must cater for different career pathways and journeys within cyber security, both technical as well as non-technical cyber security roles.
10. The scheme must set clear objectives, outcomes, and value for industry stakeholders.

STEPS TO DEVELOPING A SUCCESSFUL AUSTALIAN CYBER SECURITY PROFESSIONALISATION SCHEME

STEP ONE: ESTABLISHING A WORKING GROUP OF RELEVANT GOVERNMENT, INDUSTRY AND ACADEMIA STAKEHOLDERS

As part of developing a professionalisation scheme, it is proposed that a Professionalisation Industry Working Group be established to discuss a proposed scheme, utilising this whitepaper as a basis for discussions. For the purposes of ensuring relevance of any future scheme to government, industry, and academia, it is recommended that the working group consists of 10-15 persons and consists of individuals representing the following key industry stakeholders:

1) The Australian Information Security Association (AISA) representing the Australian cyber security profession
2) The Australian Cyber Security Growth Network (AustCyber) representing industry and government views
3) The Australian Computer Society (ACS) representing the broader views of the ICT sector
4) Representatives from Industry including notable employers in the cyber security sector.
5) Representatives from Academia including Universities and TAFEs
6) The Australian Women in Security Network (AWSN) representing the views of women in the cyber security sector
7) The Technology Council of Australia (TCA) representing the collective views of the private sector and industry in the proposed scheme

8) The Australian Information Industry Association (AIIA) which can supplement the collective views of private sector and industry in the proposed scheme.

9) Representatives from the Federal Government, specifically the Department of Industry, Science and Resources (DISR), the Australian Signals Directorate (ASD), the Department of Home Affairs (DHA) and/or the Australian Cyber Security Centre (ACSC)

STEP TWO: APPOINTING OR ESTABLISHING A GUIDANCE BODY FOR CAREER PATHWAYS IN CYBER SECURITY

To facilitate the establishment of a professionalisation scheme, it will be necessary to appoint or establish a body to administer the scheme. Such a body might be an existing organisation that is willing and suitable to perform the role. Alternatively, a body set up for the sole purpose of administering such a scheme.

The guidance body must operate cooperatively and consultatively across industry with the sole and overriding mission of upholding professional standards and ethics within the Australian cyber security sector.

Any such body that is appointed or established will need to be tasked with administering the scheme, establishing criteria for accreditation, recognising accreditation, and supervising any affiliated organisations for which the professionalisation scheme will rely on to recognise competency. The recognised guidance body should be tasked with establishing precisely what a career in cyber security could look like for individuals looking to become accredited professionals.

The Australian Information Security Association (AISA) has some degree of standing to be considered for this role. However, even within the membership of AISA, there is significant disagreement in terms of the need for professionalisation and what the model should look like should a national professionalisation scheme be adopted.[5] Additionally, AISA does not have a structured scheme for membership, nor is it a member of the Professional Standards Council. On AISA's website, it advises prospective members that 'our broad membership base consists of information security professionals from industries such as IT, software development, financial services, education, energy, utilities, telecommunications, consultant/advisory, healthcare, government, transportation, hospitality, tourism, retail, manufacturing and mining'[6] adding that 'our members range from company directors and managers to lawyers, risk professionals, software architects and highly-skilled technical security specialists'.[7] As such, there is no transparent mechanism for the assessment of individuals to any merit-based criteria for membership, with membership levels seemingly issued via a self-attestation by the individual. Similarly, it does not maintain a structured professional development scheme for members, nor does it require members to complete a minimum level of continuing professional education. As such, as AISA is currently structured, it would be an unsuitable body for such a scheme.

STEP THREE: ESTABLISHING A CYBER CAREERS PATHWAY FOR AUSTRALIAN CYBER SECURITY PROFESSIONALS

One of the tasks that the working group will need to establish is the creation, documentation, and promulgation of a formal cyber career's pathway for existing and future cyber security professionals. Significant ambiguity remains even with seasoned cyber professionals as to the steps required to be deemed a competent professional. This ambiguity is then reflected with potential cyber security professionals, who often rely on anecdotal or self-serving sources of information from institutions financially vested in signing up trainees for their own programs.

An indicative cyber careers pathway for Australian cyber security professionals which the working group should consider is provided at Figure 1.

[5] AISA, *Research into Cyber Security Accreditation in Australia, 2022*, https://aisa.org.au/common/Uploaded%20files/Research/AISA_NSW%20Report_2020_Final.pdf.

[6] AISA, *Membership – Benefits*, https://www.aisa.org.au/Public/Public/Benefits.aspx.

[7] Ibid.

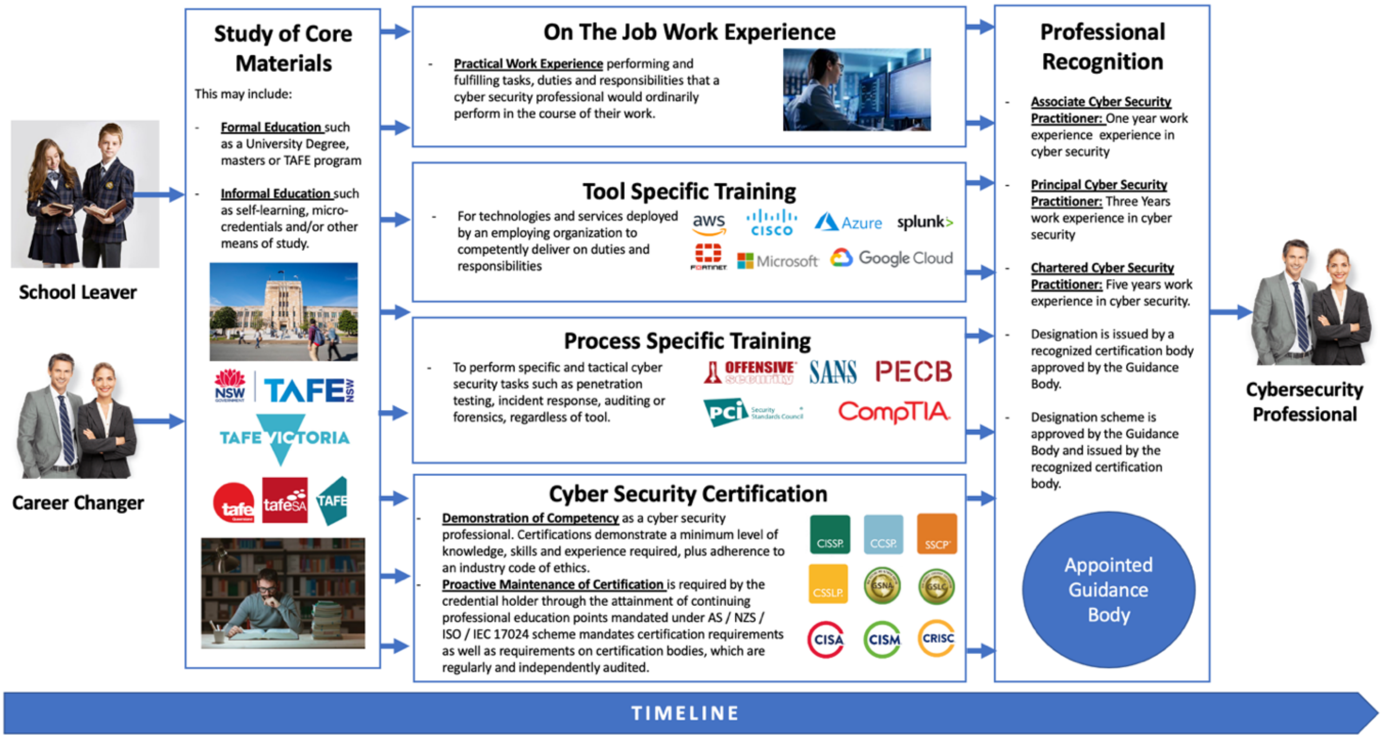
School Leaver
Career Changer
Study of Core Materials
This may include:
- Formal Education such as a University Degree, masters or TAFE program
- Informal Education such as self-learning, micro-credentials and/or other means of study.
NSW
TAFE NSW
TAFE VICTORIA
tafe
tafeSA
TAFE
On The Job Work Experience
- Practical Work Experience performing and fulfilling tasks, duties and responsibilities that a cyber security professional would ordinarily perform in the course of their work.
Tool Specific Training
- For technologies and services deployed by an employing organization to competently deliver on duties and responsibilities
aws
cisco
Azure
splunk>
FORTINET
Microsoft
Google Cloud
Process Specific Training
- To perform specific and tactical cyber security tasks such as penetration testing, incident response, auditing or forensics, regardless of tool.
OFFENSIVE security
SANS
PECB
PCI Security Standards Council
CompTIA
Cyber Security Certification
- Demonstration of Competency as a cyber security professional. Certifications demonstrate a minimum level of knowledge, skills and experience required, plus adherence to an industry code of ethics.
- Proactive Maintenance of Certification is required by the credential holder through the attainment of continuing professional education points mandated under AS / NZS / ISO / IEC 17024 scheme mandates certification requirements as well as requirements on certification bodies, which are regularly and independently audited.
CISSP
CCSP
SSCP
CSSLP
GSNA
GSLC
CISA
CISM
CRISC
Professional Recognition
- Associate Cyber Security Practitioner: One year work experience experience in cyber security
- Principal Cyber Security Practitioner: Three Years work experience in cyber security
- Chartered Cyber Security Practitioner: Five years work experience in cyber security.
- Designation is issued by a recognized certification body approved by the Guidance Body.
- Designation scheme is approved by the Guidance Body and issued by the recognized certification body.
Appointed Guidance Body
Cybersecurity Professional
TIMELINE

FIGURE 1 – A Potential Career Roadmap for Cyber Security Professionals

STEP FOUR: ESTABLISHING AN AUSTRALIAN PROFESSIONAL RECOGNITION SCHEME LEVERAGING EXISTING QUALITY CERTIFICATIONS, WORK EXPERIENCE AND TERTIARY EDUCATION

It will be necessary to establish an agreed cross-industry professionalisation scheme. It is recommended that any such scheme recognise existing and past work experience, tertiary education, recognised industry certifications, quality-assured training as well as vendor-led accreditations to minimum levels of competency pursuant to the level of professional recognition being sought, aligned to the following framework.

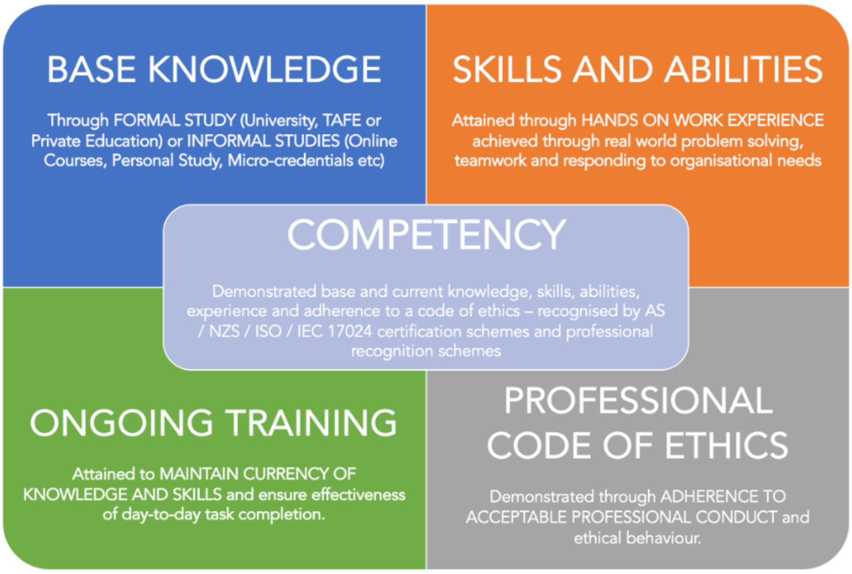
BASE KNOWLEDGE
Through FORMAL STUDY (University, TAFE or Private Education) or INFORMAL STUDIES (Online Courses, Personal Study, Micro-credentials etc)
SKILLS AND ABILITIES
Attained through HANDS ON WORK EXPERIENCE achieved through real world problem solving, teamwork and responding to organisational needs
COMPETENCY
Demonstrated base and current knowledge, skills, abilities, experience and adherence to a code of ethics – recognised by AS / NZS / ISO / IEC 17024 certification schemes and professional recognition schemes
ONGOING TRAINING
Attained to MAINTAIN CURRENCY OF KNOWLEDGE AND SKILLS and ensure effectiveness of day-to-day task completion.
PROFESSIONAL CODE OF ETHICS
Demonstrated through ADHERENCE TO ACCEPTABLE PROFESSIONAL CONDUCT and ethical behaviour.

FIGURE 2 – Elements of a Proposed Professional Recognition Scheme Framework for Australian Cyber Security Professionals

Under the proposed scheme contained within this whitepaper:

- New and/or early-stage entrants to cyber security would be graded as Associate Cyber Security Professionals.
- Established practitioners with formal education and some work experience would be graded as Principal Cyber Security Professionals.
- Senior practitioners with extensive work experience would be designated as Chartered Cyber Security Professionals.

Professionalisation levels would be based on competency assessed against candidate knowledge, skills, and experience, with this model following from the work currently being considered by the UK Government through the UK Cyber Security Council[8] in the proposed professionalisation scheme being considered and implemented for the UK cyber ecosystem.

The proposed scheme includes two tracks which an individual can accredit to: a 'fast track' approach using AS / NZS / ISO / IEC 17024 recognised industry certifications which validate knowledge, skills and experience attributes would be included; and a points-based approach for those who do not hold such certifications which would see points awarded based on tertiary education, vendor certifications / accreditations, hands on work experience and a background / character check through law enforcement.

The number of points attributed to tertiary education courses would be based on the quality of the course and its relevance to the needs of industry and the community. These courses would need to be recognised and assessed by the guidance body before they are included into the scheme. This will help ensure tertiary courses continually improve and are responsive to the needs of industry, responding to rapid changes in cyber security. It is envisaged that such an approach would reward industry education providers who can deliver valuable, relevant, and current education courses for the cyber security sector. Years of service in cyber security roles would also be attributed points based on type and length of service.

Proposed Professional Recognition Level	**Description of Recognition Level with Career Stage**	**Equivalent Years of Demonstrated Work Experience**
Associate Cyber Security Professional	New Entrant to Early Career	0 to 2 Years
Principal Cyber Security Professional	Early Career to Mid-Career	2 to 5 Years
Chartered Cyber Security Professional	Mid-Career to Senior Career	5 Years +

Table 1 – Proposed Professional Recognition Levels to Career Stage and Equivalent Years of Demonstrated Work Experience

STEP FIVE: EVALUATING THE ROLE OF EXISTING INDUSTRY CERTIFICATIONS IN THE PROPOSED PROFESSIONAL RECOGNITION SCHEME

An essential element of professional recognition will be to consider the numerous education offerings available as well as personnel accreditation schemes that already exist and operate successfully within the Australian cyber security ecosystem. While these offerings differ in nature and quality, many, particularly recognised certifications, enjoy broad industry appeal, with prestige in some of these schemes anchored in independent and verifiable quality control standards such as AS / NZS / ISO / IEC 17024, the international standard which governs and formalised accreditation and certification of individuals. Under this standard, accreditation is based on a candidate's levels of competency, including demonstrated levels of knowledge, skills, and relevant work experience; endorsement by an existing certified professional or by the certification body itself; adherence to a strict and professional code of ethics; and maintenance of the certification by the individual through earning continuing professional education. Additionally, a formalised process in determining credential knowledge areas and updating accredited certifications on a periodic basis are core to the AS / NZS / ISO / IEC 17024 standard. For these reasons, AS / NZS / ISO / IEC 17024 certifications have been recognised and are incorporated into numerous accreditation, certification, and recognition schemes, here in Australia as well as globally. It should be noted that AS / NZS / ISO / IEC 17024 certifications are often used by employers as a measure of an individual's knowledge, skills, abilities and experience when recruiting staff. For example, the (ISC)^2 CISSP certification is listed as a requirement or as desirable for over 5,700 open roles in Australia as of January 2023.[9] Similarly, the ISACA CISA is listed as a requirement or as desirable for over 900 open roles in Australia.[10]

It must be noted that in Australia, the ASD Independent Registered Assessors Program (IRAP) program recognises AS / NZS / ISO / IEC 17024 certifications as prequalifiers to IRAP accreditation, specifically the (ISC)^2 CISSP; ISACA CISM, CISA and CRISC; the GIAC GSLC and GSNA; the PECB ISO 27001 Lead Auditor and the PCI QSA.[11] Additionally, AS / NZS / ISO / IEC 17024 accredited certifications are recognised by international partners in the U.S. via the US Department of Defence 8570.01-M / 8140.01 standards, the UK Government endorsed Certified Cyber Professional (CCP) Assured Service administered by the British Computer Society (BCS) and the Chartered Institute of Information Security (CIISec).

[8] The UK Cyber Security Council, https://www.ukcybersecuritycouncil.org.uk/

[9] LinkedIn, *Job Search – keyword 'CISSP'*, https://www.linkedin.com/jobs/search/?currentJobId=3354208037&keywords=cissp&refresh=true.

[10] LinkedIn, *Job Search – keyword 'CISA'*, https://www.linkedin.com/jobs/search/?currentJobId=3365456763&geoId=101452733&keywords=cisa&location=Australia&refresh=true/.

[11] ACSC, *IRAP Application Form*, https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-application-form#no-back.

STEP SIX: EVALUATING THE ROLE OF TERTIARY EDUCATION IN THE PROPOSED PROFESSIONAL RECOGNITION SCHEME

A traditional route into the cyber security sector involves individuals completing a recognised degree program via an Australian (or overseas) university or via a TAFE accreditation. At university, this can often involve a Computer Science, Information Technology, or a dedicated Cyber Security degree, either at undergraduate or postgraduate level. At TAFE, a Certificate III/IV in Information Technology, Networking or Cyber Security is also well recognised. This whitepaper contends that a professional recognition scheme needs to incorporate recognition of such programs, coupled with the requirement that an individual seeking accreditation possess a minimum amount of paid and verifiable work experience as a cyber security practitioner.

STEP SEVEN: ESTABLISHING THE ROLE OF PAID AND VERIFIABLE WORK EXPERIENCE IN THE PROPOSED PROFESSIONALISATION RECOGNITION SCHEME

A concern often vocalised by industry is that it requires competent individuals who possess paid and verifiable work experience with cyber security. It is for this reason that AS / NZS / ISO / IEC 17024 industry accreditations which require paid and verifiable work experience have earned considerable respect as an indicator of an individual's competency in the field, and why many job descriptions include a desired listing of industry certifications. It is validly noted and recognised that for those who do not have, or have very limited work experience, this is a limiting factor in terms of employment prospects. As part of the proposed recognition scheme, it is contended that the formal recognition of paid work experience is an essential element for individuals who may or may not possess academic qualifications or AS / NZS / ISO / IEC 17024 industry accreditations.

STEP EIGHT: ALIGNING DEVELOPMENT PATHWAYS CREATED FOR INTERNATIONAL SKILLED MIGRANTS AND INTERNATIONAL GRADUATES IN CYBER SECURITY OF AUSTRALIAN UNIVERSITIES WITH THOSE DISCUSSED ABOVE.

No current scheme exists to support new permanent residents and skilled migrants in securing their first jobs and particularly where they have background equipping them to work with ADF, police or banks. This task needs to be undertaken by the new guidance body discussed in earlier steps, in conjunction with the relevant skills recognition branch of the Department of Education so as to understand the nature of the applicant's original studies and where it equips them for cyber security employment within an Australian context.

THE PROPOSED METHODOLOGY TO BE EMPLOYED IN ASSESSING INDIVIDUALS TO ATTAIN PROFESSIONAL RECOGNITION UNDER THIS SCHEME

It is proposed that two specific pathways to cyber security professionalisation are incorporated as part of a future Australian cyber security professionalisation scheme. Under both pathways, an appointed and recognised Australian cyber security industry body would become the recognised guidance body and authority for Australian cyber security professionals.

PATHWAY ONE: FAST TRACK USING AS / NZS / ISO / IEC 17024 COMPLIANT ACCREDITATIONS

The recognised Australian cyber security industry authority and guidance body would formally accredit relevant international certifications to denote professional recognition for Australian cyber security professionals in line with the professionalisation scheme. Eligible certifications would be limited to those issued by relevant not-for-profit cyber security industry bodies and only to those that are AS / NZS / ISO / IEC 17024 accredited certifications. AS / NZS / ISO / IEC 17024 is critical as it demonstrates that accredited certifications follow a verifiable and structured process for individuals to accredit against, which incorporate knowledge, skills, experience, and adherence to a code of ethics. The approved Australian guidance body would categorise certifications issued by these international bodies according to the level of competence each certification demonstrates and bestow the title of *Associate*, *Principal* or *Chartered* pursuant to that level of certification. For individuals using AS / NZS / ISO / IEC 17024 certifications as a basis for their professional recognition, individuals would need to remain compliant and current with their internationally issued industry certifications to maintain currency under the proposed Australian professionalisation scheme.

In seeking to create a professionalisation scheme, in the immediate term, it would be wise to take into consideration the existing accreditation landscape, particularly those administered under AS / NZS / ISO / IEC 17024. This will ensure that the new scheme can be rapidly adopted by an existing and significantly sized cohort of individuals who are already certified in internationally recognised, industry-respected, and quality-controlled certifications. Crucially, the strict and formalised process which each certification body must adhere to for the regular updating of the bodies of knowledge underpinning each certification ensures that the both the certification as well as any scheme that relies on those certifications remains futureproofed. Similarly, the requirement that certified individuals accredited under AS / NZS / ISO / IEC 17024 maintain their certifications through a formalised process of continuing professional development and education ensures that individuals who maintain their certifications can demonstrate currency of knowledge, skills, experience, and overall competency, providing an additional layer of validity and relevance to any schemes that use AS / NZS / ISO / IEC 17024 accreditations as a basis for recognition.

Certification	**Verified Work Experience Requirements**	**Accreditation Status Claimable**
(ISC)^2		
CISSP	5 Years	Chartered
CISSP-ISSAP	6 Years	Chartered
CISSP-ISSEP	6 Years	Chartered
CISSP-ISSAP	6 Years	Chartered
CCSP	5 Years	Chartered
SSCP	1 Year	Associate
CSSLP	4 Years	Principal
ISACA		
CISM	5 Years	Chartered
CISA	5 Years	Chartered
CRISC	3 Years	Principal
CPDSE	3 Years	Principal
CGEIT	5 Years	Chartered
CompTIA		
Security+	1 Year	Associate
CySA+	4 Years	Principal
Pentest+	3 Years	Principal
PECB		
ISO 27001 Implementer	2 Years	Associate
ISO 27001 Lead Implementer	5 Years	Principal
ISO 27001 Senior Lead Implementer	10 Years	Chartered
ISO 27001 Auditor	2 Years	Associate
ISO 27001 Lead Auditor	5 Years	Principal
ISO 27001 Senior Lead Auditor	10 Years	Chartered

Table 2 – Proposed Categorisation of selected recognised AS / NZS / ISO / IEC 17024 certifications against the proposed Australian Professionalisation Scheme. This is not an exhaustive or final list of proposed certifications to be used for a 'fast track' scheme, however, any potential certification on the 'fast track' scheme must be AS / NZS / ISO / IEC 17024 accredited to qualify for inclusion by the proposed Guidance Body.

PATHWAY TWO: A DEMONSTRATION OF COMPETENCY-BASED ATTRIBUTES FOR PROFESSIONAL RECOGNITION UNDER THE PROPOSED SCHEME.

For individuals seeking professional recognition who may not hold a recognised AS / NZS / ISO / IEC 17024 certification or accreditation under Pathway One, nor seek to undertake such an accreditation, the recognised Australian authority and guidance body for Australian cybersecurity professionals would utilise a credit points system whereby credits are awarded based on an individual's verified knowledge, skills, education, and experience. Credits will vary based on the type of education, experience and training being claimed. The approved guidance body would then categorise individuals according to the level of competence demonstrated, bestowing the title of *Associate*, *Principal* or *Chartered* pursuant to that level of competence.

Individuals accredited under this pathway will be required to maintain their professional accreditation by demonstrating ongoing education and currency of skills through a Continuing Professional Education and Development (CPE / CPD) scheme administered by the recognised Australian guidance body, equivalent in nature and rigour to that defined under AS / NZS / ISO / IEC 17024. This scheme will need to be operated by the recognised Australian guidance body.

It is understood and appreciated that there are numerous routes that an individual could take into the cyber security profession, both conventional as well as non-conventional. Some individuals may create their own career journey and demonstrate an equally valuable set of knowledge, skills, experience, and competency. This pathway caters for such individuals. For the purposes of illustrating how a potential professionalisation scheme could operate, credits could be assigned for indicators of competency, such as a tertiary education program in or directly related to cyber security. A limited and provisional example schedule of credits for each indicator of competency is listed below.

INDICATOR OF COMPETENCY	CREDITS
Tertiary Educational Programs Recognised by the Guidance Body	
TAFE Cert III / IV in Cyber Security (or Equivalent)	10
TAFE Cert III / IV in IT and related fields (for example: network and systems administration)	5
Recognised Diploma or Advanced Diploma in Cyber Security	10
Recognised Diploma or Advanced Diploma in IT and related fields (for example: network and systems administration)	5
Recognised Bachelor's Degree in Cyber Security	30
Recognised Bachelor's Degree in IT	20
Recognised Master's Degree in Cyber Security	30
Recognised Master's Degree in IT	20
PhD in Cyber Security	20
Note: It would be the work of the guidance body (as a Professional Standards Body operating per Australian legislation) to assert how recognised Tertiary Education Programs could contain elements of the following disciplines, derived under the Cyber Security Body of Knowledge (CyBOK)[12] as defined below, or similar recognised work such as the IEEE Cyber Security Framework that is currently recommended by the ACS. Human, Organisational and Regulatory Aspects of Cyber Security o Risk Management and Governance o Law and Regulation o Human Factors of Cyber Security o Privacy and Online Rights Attacks and Defences o Malware and Attack Technologies o Adversarial Behaviours o Security Operations and Incident Management o Forensics Systems Security o Cryptography o Operating Systems and Virtualisation Security o Distributed Systems Security o Formal Methods for Security o Authentication, Authorisation and Accountability Software and Platform Security o Software Security o Web and Mobile Security o Secure Software Lifecycle Infrastructure Security o Applied Cryptography o Network Security o Hardware Security	

[12] *CyBOK: Cyber Security Body of Knowledge*, University of Bristol (UK), https://www.cybok.org/knowledgebase1_1/.

○ Cyber Physical Systems ○ Physical Layer and Telecommunication Security	
Recognised Vendor Accreditations Approved by the Guidance Body	
Vendor issued AS / NZS / ISO / IEC 17024 accreditations that are not issued by recognised international not-for-profit industry associations. Examples may include: • Cisco CCNA and CCNP. • EC-Council CCISO, CEH, CND, CHFI and ECIH.	Between 10 and 20 depending on the nature of the accreditation
Vendor issued non-AS / NZS / ISO / IEC 17024 recognised credentials Examples may include: • AWS Certified Certifications: AWS Certified Cloud Practitioner, for example • Microsoft Certifications: SC-900 Microsoft Certified in Security Compliance and Identity Fundamentals, for example • SANS Institute: SEC504: Hacker Tools, Techniques and Incident Handling, for example. • Offensive Security: OSCP, OSCE, OSEE, OWSE for example • eLearnSecurity: eJPT, eCPPT, eCPTX, eWPT for example.	Between 5 and 20 depending on quality and content.
Work Experience Formally Recognised by the Guidance Body	
Each Equivalent Full Time Year of Paid and Verifiable Work Experience in Cyber Security Note: Any recognised work experience must include at least one element of the following disciplines within the cyber security ecosystem derived under the Cyber Security Body of Knowledge (CyBOK):[13] or other recommended model. Human, Organisational and Regulatory Aspects of Cyber Security ○ Risk Management and Governance ○ Law and Regulation ○ Human Factors of Cyber Security ○ Privacy and Online Rights Attacks and Defences ○ Malware and Attack Technologies ○ Adversarial Behaviours ○ Security Operations and Incident Management ○ Forensics Systems Security ○ Cryptography ○ Operating Systems and Virtualisation Security ○ Distributed Systems Security ○ Formal Methods for Security ○ Authentication, Authorisation and Accountability Software and Platform Security ○ Software Security ○ Web and Mobile Security ○ Secure Software Lifecycle Infrastructure Security ○ Applied Cryptography ○ Network Security ○ Hardware Security ○ Cyber Physical Systems ○ Physical Layer and Telecommunication Security	10

TABLE 3 – Proposed Indicators of Competency with indicative credit weightings for selected education programs. This is not an exhaustive or final list of proposed indicators of competency to be used for a 'credit point' scheme. Additionally, the credit point weightings attributable to each indicator of competency will need to be finalised prior to implementation of a scheme. However, any potential indicator of competency on the 'credit point' scheme must be approved by the proposed Guidance Body to qualify.

Subject to formal background and character verification undertaken by the guidance body, under a proposed scheme operating under the competency-based method:

- an individual seeking to attain *Associate* status would require 20 credits.
- an individual seeking to attain *Principal* status would require 50 credits.
- an individual seeking to attain *Chartered* status would require 100 credits.

[13] *CyBOK: Cyber Security Body of Knowledge*, University of Bristol (UK), https://www.cybok.org/knowledgebase1_1/.

MAPPING THE PROPOSED PROFESSIONAL ACCREDITATION SCHEME TO EXISTING AUSTRALIAN GOVERNMENT PROFICIENCY LEVELS

It is noted that the Australian government employs several schemes to indicate competency levels, including the ASD Cyber Skills Framework.[14]

To facilitate better acceptance of the proposed Accreditation Scheme, an indicative mapping of accreditations to existing schemes is as follows:

PROPOSED AUSTRALIAN CYBER SECURITY PROFESSIONALISATION RECOGNITION SCHEME	ASD CYBER SKILLS FRAMEWORK LEVEL	CIISEC SKILLS FRAMEWORK	SFIA LEVELS	ASD STREAMS
Associate	Level 1 – Learner	Level 1 – Knowledge	Level 1 – Follow	N/A
	Level 2 – Novice	Level 2 – Knowledge and Understanding	Level 2 – Assist	Level 1 – Novice
Principal	Level 3 - Practitioner	Level 3 – Apply	Level 3 – Apply	Level 2 – Practitioner
	Level 4 – Senior Practitioner	Level 4 – Enable	Level 4 – Enable	
Chartered	Level 5 – Principal Practitioner	Level 5 – Advise	Level 5 – Advise, Ensure	Level 3 – Expert
	Level 6 – Expert Practitioner	Level 6 – Expert	Level 6 – Initiate, Influence Level 7 – Set Strategy, Inspire, Mobilise	Level 4 - Leader

TABLE 4 – Indicative Mapping of Accreditation Scheme Status (Associate, Principled, Chartered) with Australian Cyber Ecosystem Frameworks and Standards

CONCLUSION

The Australian cyber security industry sits at a crossroads, one which more established industries have endured in their own histories. Faced with challenges which have undermined those sectors, visionary professionals in those sectors agreed that reform was needed and established professionalisation schemes to ensure that both industry and members of the public could identify credentialed and competent individuals to assist them with their problems and challenges.

The time for professionalisation of the Australian cyber security sector has come: to provide entrants into the sector a level of certainty as to what is needed to achieve their career goals; to provide academia a pathway to credible and relevant education offerings; to provide industry and the private sector the ability to discern which individuals have achieved a base level of competence in cyber security; to provide a framework and a governance model for cyber professionals and their continuing education requirements; and finally to help achieve a safer and more cyber secure Australia.

[14] ASD, *ASD Cyber Skills Framework,* https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf

ABOUT THE AUTHORS

Tony Vizza has been involved in the information technology, information security and privacy fields for more than 25 years.

Tony has completed a Bachelor of Science in Computing Science from the University of Technology, Sydney and a Global Executive MBA from the University of Sydney which included study at Stanford University in the United States, The London School of Economics in the UK and the Indian Institute of Management, Bangalore in India. Tony is currently studying for a Juris Doctor law degree at the University of New South Wales. Tony's information security credentials include the CISSP (Certified Information Systems Security Professional), CCSP (Certified Cloud Security Professional), CIPP/E (Certified Information Privacy Professional / Europe), CRISC (Certified in Risk and Information Systems Controls), CISM (Certified Information Security Manager) and he is a certified ISO/IEC 27001 Senior Lead Auditor.

Tony is a Cyber Security Ambassador for the NSW Government, a member of the Cybersecurity Industry Advisory Committee for the NSW Government, a member of the Technology and Business Services Industry Skills Reference Group for NSW TAFE, a member of the Data Security Standards Committee for Blockchain Australia, and has provided expert services to the United States Government Department of Energy (DoE), the United Kingdom Department of Culture, Media and Sport (DCMS), the European Union Cyber Security Organisation (ECSO), the Australian Government's Australian Prudential Regulation Authority (APRA), the Australian Signals Directorate (ASD), the Law Society of NSW, the Australian Security Industry Association Limited (ASIAL), the Australian Institute of Project Management (AIPM) as well as numerous boards. Tony served as a Director of the Board for the Australian Information Security Association (AISA) from 2020 to 2022. Tony is currently an Executive Director with KordaMentha, leading the cyber security advisory and risk management practice, providing expert cyber security advisory, forensic and incident response services to Australian organisations in the private and public sector.

Tony is an expert speaker on information security regularly speaking across the world on information security matters. He has also taught and mentored young and aspiring information security students through Victoria University, TAFE NSW and TAFE Victoria in association with Infoxchange and has lectured cybersecurity students at the University of Technology, Sydney, the University of New South Wales and the University of Queensland. Tony is also a regular contributor to numerous cyber security and IT industry publications including CSO Magazine, Infosecurity Magazine, Cyber Today Australia, Security Insider Magazine, Australian Reseller News (ARN), Channel Reseller News (CRN) and Lifehacker, amongst others, regarding information security, privacy, business, and channel strategy.

Professor Jill Slay AM is the University of South Australia SmartSat Cooperative Research Centre Professorial Chair in Cybersecurity. She has twenty-two years of experience in the development of cyber security standards and accreditation gained from her association with (ISC)^2 and Idaho State and Johns Hopkins Universities. Her work has informed Australian policy in cyber security, digital forensics and critical infrastructure protection and developed operational understanding and training equipment for the ADF and the Australian Signals Directorate who were partners on some of her research. She has advised politicians of all parties. She worked with Major General Marcus Thompson, recently retired Chief of Information Warfare, previously Head of Signals Corps, who led all national cyber security/warfare research and development for the Australian Defence Force (ADF) from 2016-2020 and who has been an adjunct researcher with her since he graduated with his PhD under her supervision.

Her academic research focuses on the context of developing the national technical agenda in satellite cybersecurity and resilience with the Australian Defence Science and Technology Group, Defence and Defence Industry. She is ranked as being in the top 2% of scientists in the world in ICT Networking and Telecommunications sub field (in 2019) as an early adopter of AI and Machine Learning in Cyber Security and Real Time Forensics. She applies these techniques to satellite security.

She is a Vice-Chair of the Board of the International Information Systems Security Certification Consortium (ISC)^2 for 2021-2023. Previous appointments have included Optus Chair in Cybersecurity at La Trobe University and Founding Director of the Australian Centre for Cyber Security at the Australian Defence Force Academy. She has established an international research reputation in cyber security (particularly Digital Forensics, Cyber Intelligence and Cyberwarfare) and has worked in collaboration with the Australian Federal and State governments and with many industry partners. She has published more than 180 outputs in information assurance, critical infrastructure protection, security and forensic computing and completed the supervision of 22 PhDs with 7 others ongoing, and many master's and Honour's theses. She was made a Member of the Order of Australia (AM) for service to the information technology industry through contributions in the areas of forensic computer science, security, protection of infrastructure and cyber-terrorism

LEGAL INFORMATION

1. The views and opinions expressed in this document are those of the authors and do not necessarily reflect the official policy or position of any entity referred to within this document. Examples of analysis performed within this document are only examples.
2. While care and consideration has been taken in the creation of the material in this document, the authors do not warrant, represent, or guarantee that the material published in this document is in all respects accurate, complete, and current. To the fullest extent permitted by law, any liability, including any liability for negligence, for any loss or damage arising from reliance on material in this document, is excluded.
3. Except as permitted by copyright law, you may not reproduce or communicate any of the content in this document, without the express permission of the copyright owner.
4. The Australian Copyright Act allows certain uses of content without the copyright owner's permission. This includes uses by educational institutions for educational purposes and by Commonwealth and State government departments for government purposes, provided fair payment is made.

KordaMentha

Contact us

Brisbane	+61 7 3338 0222
Jakarta	+62 21 3972 7000
Melbourne	+61 3 8623 3333
Perth	+61 8 9220 9333
Singapore	+65 6593 9333
Sydney	+61 2 8257 3000
Townsville	+61 7 4724 9888

For more information visit
kordamentha.com

Liability limited by a scheme approved
under Professional Standards Legislation.