Australia's Cyber Security Strategy 2023-2030

AMAZON WEB SERVICES SUBMISSION

Introduction

Amazon Web Services (AWS) is pleased to comment on *Australia's Cyber Security Strategy 2023-2030 Discussion Paper*. We welcome the ambitious vision for the new Strategy, reflecting the real challenges posed by cyber-enabled risks. Security has always been our top priority at AWS and we believe that, into the future, thinking about and dealing with cybersecurity will be a cornerstone of modern life.

The case for government's focus on cybersecurity is clear. Cybersecurity is a pressing economic and societal challenge that impacts all facets of modern life. The World Economic Forum's *Global Risk Report 2023* lists cybercrime and cyber insecurity as number 8 out of its Top 10 risks, over both the short and longer term. In Australia, estimates on the costs of cybercrime vary, but as of 2021 the ACSC reported annual self-reported financial losses of more than $33 billion. For individuals, the psychological toll of falling victim to cybercrime is only beginning to be understood, especially at a time where online communication has become the primary means of staying connected and doing business.

This might seem like a gloomy outlook, but we see cause for optimism. The rapid acceleration of digital transformation in a short time has forced organisations to more proactively manage and assess disruptions to their business, expediting the transition away from legacy IT infrastructure and resulting in significant operational improvements that create substantial security benefits. Instead of seeing security as a separate function, tacked on at the end of a process and slowing innovation, we see strong security increasingly treated as a core business enabler.

Challenges clearly remain. At its core, cybersecurity is a macro-level challenge made up of a seemingly endless number of micro-level problems. The evolving security and regulatory landscapes leave many entities feeling overwhelmed. Their limited security teams – *if* they're resourced to have a dedicated security team – are already working at bandwidth, and need to be able to assure their leadership that their organisation is managing its cybersecurity risks. At the same time, a global shortage of security professionals exacerbates workforce limitations. For small and medium businesses, and individuals, these challenges are even more profound. Cybersecurity can seem like an insurmountable objective.

AWS believes this perception can and must shift. Our response to the Discussion Paper is grounded in the following tenets, which we see as essential for the success of a new Strategy. We believe a new Strategy should:

Simplify the message. Defuse and demystify the language around cybersecurity to make it more accessible, achievable, and empowering.

Cover the basics. Provide clarity and support to businesses and individuals on the fundamentals of cybersecurity, including strong governance and hygiene practices.

Establish technical grounding. Initiatives should be grounded in evidence and appropriately reflect the risks and as well as the benefits of different technologies.

Future proof through flexibility. Ensure that policies, guidance and frameworks are flexible and remain fit-for-purpose as technologies evolve.

Promote a culture of partnership. Foster purpose-driven collaboration that is outcome-focused and aligned to strategic objectives.

Avoid boiling the ocean. Maintain clarity of purpose and focus on big picture issues that have impact at a national level.

In our submission, we are focusing on the elements of cybersecurity that sit outside the realm of intelligence agencies, law enforcement, and Defence. These are important subjects, and we welcome the opportunity to engage more deeply with Government on these areas in a forum more appropriate to their level of sensitivity. The focus of our submission is, instead, on the elements of security that comfortably sit in the open.

We welcome ongoing engagement with Government as it develops the new Strategy.

Best regards,

[redacted]
Head of Public Policy, Australia and New Zealand
Amazon Web Services

Summary of Recommendations

Recommendation 1: Consider designing a world-first 'Safe System' approach for cyber security. Inspired by the Vision Zero road safety strategy, develop a Cyber Safe System for a systematised, integrated, and multi-disciplinary approach to cybersecurity. AWS would be pleased to support this initiative.

Recommendation 2: Consciously simplify the language around cybersecurity to make it more accessible, achievable, and empowering. Shift from alarmist and overly technical rhetoric to help small entities and individuals feel empowered to manage their cyber risks effectively, while encouraging transitions to more secure and resilient technologies.

Recommendation 3: Government co-creates and publishes secure-by-design principles with industry that takes a flexible and user-centric approach. Technology is not static – we operate in a dynamic security environment that needs to constantly adapt to new technologies, new designs, and new ways of working. Laying out clear, actionable principles for what it means to be secure-by-design in different contexts is one step government can take to support the whole of the Australian economy.

Recommendation 4: Government conducts deep consultations on the development of a robust digital ID framework based on foundational and infrastructural models, as a matter of priority. AWS welcomes the announcement following the February meeting of the Digital and Data Ministers of shared intent between the states, territories, and Commonwealth to strengthen Australia's digital identity framework, and we look forward to engaging deeply on this topic.

Recommendation 5: Government emphasise and promote Multi-factor authentication (MFA) as a 'one essential activity' for organisations and users. Although MFA is one of the Top Four strategies in the ACSC's Information Security Manual, there is a compelling case for it to be the most actively promoted activity, for entities and individuals alike.

Recommendation 6: Government partner with industry and academia to develop best practice guidance for data governance and management as part of a holistic approach to data protection. AWS sees an important opportunity for the Australian Government to address a genuine policy gap through a clearly articulated approach to data governance and data management.

Recommendation 7: Government conduct an audit of existing programs intended for small and medium-sized businesses (SMBs), and consolidate the initiatives into a program modelled on the UK's Cyber Essentials. We encourage the Australian Government to take a long-term, evidence-based view to maximising the impact of its support programs for SMBs. AWS would be proud to support government in creating actionable guidance for SMBs on safe digitisation.

Recommendation 8: Government partner with industry to create a national mentor program in cybersecurity. Creating workplaces that not only welcome, but celebrate and understand the value

of diversity, requires ongoing and systemic cultural change. We need to encourage this change through the development of future staff through mentorship programs, and by connecting with the future generations of the workforce.

Recommendation 9: Cybersecurity education and training should be integrated into school curriculums and non-cybersecurity university and TAFE programs. Cybersecurity is a feature of modern life, and having a cybersecurity literate society and broader workforce is equally important for reducing risks over time. AWS would be proud to contribute to this nationwide effort.

Recommendation 10: Government encourage and support the development and use of automation technologies for the purpose of cybersecurity improvements. Automation is already helping to create an environment where it's easier to make the best cybersecurity decisions earlier in the development of business processes and digital products. This, however, depends on major modernisation efforts.

Recommendation 11: Government partner with industry, academia and professional associations to develop guidance that helps boards and senior executives understand how to incorporate cyber risks into investment cycles. Effectively integrating cybersecurity into all business decisions will take time – and, in many cases, will necessitate a rethink of well-worn investment processes. We encourage the Australian Government to partner with industry, academia and professional associations to foster a risk and resilience culture that encourages, rather than inhibits, digital transformation.

Recommendation 12: Government partner with industry, academia and professional associations to develop a new, fit-for-purpose funding model for digital infrastructure and software investments. Traditional 'plan, build, run' IT operations and capex-based funding models are ineffective in creating the continuous feedback and improvement loops necessary for operational excellence and, as a result, these old methods hinder substantial security improvements. We would welcome the opportunity to dive deeper on this important issue with government, which would have significant economic and cybersecurity benefits.

Recommendation 13: Allow time to implement and assess recent, ongoing or existing legislative and regulatory reforms, frameworks and programs before significantly changing those measures or introducing additional regulatory measures or compliance programs. Government has an important role to play in creating a cybersafe ecosystem through regulatory measures, the creation of incentives, building awareness across the whole of society, and providing guidance.

Recommendation 14: The existing legislative and regulatory environment applicable to cybersecurity, privacy and data protection should be simplified and harmonised into a single federal framework. To ensure consistency, avoid confusion and maintain a common language and understanding of cybersecurity, privacy and data protection expectations, a harmonisation and simplification of the regulatory environment would be beneficial to both business and government.

Recommendation 15: Any new obligations or regulatory measures should be principles-based to give entities necessary flexibility to appropriately manage their unique circumstances and security risks, and to ensure that these changes are future-proofed as much as possible. Achieving these outcomes requires consistency and clarity, balanced with necessary flexibility.

Recommendation 16: Government consider the creation of a Technical Advisory Committee for cybersecurity and adjacent areas of policy. We believe it is essential that there is a dedicated, independent statutory authority with the focus and necessary technical expertise to oversee Australia's cybersecurity framework as government continues to grapple with the policy challenges posed by technological change, particularly on the question of technical feasibility.

Recommendation 17: Government should partner with industry, academia and professional associations to develop guidance that helps boards and senior executives understand how to manage cyber risks and their obligations and responsibilities. At its core, cybersecurity is a business risk, and is already part of a director's existing duties. AWS supports the creation of guidance to help boards in understanding how to engage with cybersecurity risks, rather than imposing new and highly specific obligations on directors.

Recommendation 18: Government consolidate cyber incident reporting into a single portal, and should consider consolidating reporting requirements for other security-related regulatory regimes. The existing requirements create substantial regulatory duplication for reporting entities, and mean that sensitive information is widely dispersed, creating its own potential security risks.

Recommendation 19: Government does not expand incident reporting obligations until existing measures have been allowed more time to mature and be fully implemented, and their value has been fully assessed. The current obligations require time to mature and be fully implemented, and government should focus on assessing the value derived from current incident reporting before expanding the regime.

Recommendation 20: The Strategy considers how to fully utilise the Trusted Information Sharing Network (TISN) as a mechanism for outcome-driven industry engagement. We strongly encourage the new Strategy to consider existing forums – particularly the TISN – as a means of developing shared objectives between government and industry to meet common challenges.

Recommendation 21: The new National Cyber Security Coordinator and their Office play a substantial role in facilitating ongoing and purposeful engagement with industry to define and address strategic cybersecurity objectives. It is vitally important that, for the purposes of meeting the ambitions of the new Strategy, consultation and engagement does not stop with the submission of consultation papers.

Recommendation 22: Government create a secure data lake of threat information, allowing entities to directly query and, if they choose, share anonymised information to the platform. Threat intelligence is important, but many entities do not have the internal integrations necessary to make use of technical threat intelligence. The creation of a secure data lake by government would

allow entities to interrogate and draw on available indicators for the purposes of threat research and discovery.

Recommendation 23: Government works with industry to develop a program relating to 'threat treatment' that assesses blocking capacity, but also considers isolation, investigation, and remediation actions within risk tolerances. Threat blocking is something that requires extensive consultation and must have strong technical grounding. We would welcome the opportunity to workshop a holistic approach to threat treatment with Government as part of the development of the Strategy.

Recommendation 24: Government initiates a separate consultation for the foreign policy elements of the Strategy. While it is useful to have an international dimension included in the new Strategy to ensure strategic alignment, we believe it would be helpful to have a separate mechanism for international engagement to maintain momentum and focus in this space.

Recommendation 25: As part of a regional resilience plan, Government prioritise broader foundational capacity building and take a holistic view of resilience to disruptive events. We see scope for government to better integrate industry into key conversations with regional partners to help improve regional cyber resilience, including opportunities to collaborate on capacity building programs.

Recommendation 26: Government work with industry and academia to develop a set of priorities for cyber and tech standards, followed by an action plan for ongoing engagement. AWS recommends that Government develop a set of priorities (and priority standards forums) for cyber and tech standards and work in partnership with industry and academia to develop a targeted action plan for engagement. A mechanism for ongoing collaboration should also be established, which would include government, industry and academic experts and practitioners.

Recommendation 27: Government work to establish an AUKUS Mutual Recognition Scheme for government hosting frameworks. A mutual recognition program would substantially reduce regulatory duplication, and provide an opening for Australian entities to operate internationally.

Recommendation 28: The Strategy clearly articulates interactions with other key areas of tech policy, such as the Critical Technologies List, and links key concepts such as secure by design and continuous assurance to these policy programs. Cybersecurity should be incorporated as a key consideration for adjacent policy programs, in line with a systems-thinking approach.

Contents

Culture Gear Shift

At face value, road safety and cybersecurity might seem an unlikely policy analogy. Of course, there are obvious differences – no analogy is perfect. But we see clear parallels and learning pathways that can be applied in cyberspace. Like cybersecurity, road safety is a common international challenge. No country is immune from road-based risks, in the same way accelerating digitisation is embedding cyber-based risks across almost every aspect of society. Both issues demand a holistic policy response, ranging from end-user education, to safeguards, to infrastructure improvements.

Learn by Example

Vision Zero is a global strategy with the stated aims of eliminating traffic fatalities and severe injuries, while increasing safe, healthy, and equitable mobility. AWS has been a supporter of this program, using our Working Backwards approach with partner cities to identify projects that lead to improved safety outcomes. The Vision Zero strategy, first implemented in Sweden in the 1990s, is now a major feature of road safety programs worldwide and is the basis for Australia's National Road Safety Strategy. Consider this table produced by the Vision Zero Network:

Traditional Approach	Vision Zero
Traffic deaths are inevitable	Traffic deaths are preventable
Perfect human behaviour	Integrate human failing in approach
Prevent collisions	Prevent fatal and severe crashes
Individual responsibility	Systems approach
Saving lives is expensive	Saving lives is not expensive

Borrowing from this thinking, we can conceptualise a new way of approaching cybersecurity at a national policy level to effect consistent, meaningful change:

Traditional Approach	Cyber Safe System
Breaches are inevitable	Breaches are preventable
Perfect human behaviour	Integrate human failing in approach
Prevent incidents	Prevent serious incidents
Individual responsibility	Systems approach
Cybersecurity is expensive	Cybersecurity is not expensive

There are two key strengths in the Safe System approach, both of which can be easily adapted to thinking around cybersecurity. First is the inherent understanding that people will sometimes make mistakes (organisations are, after all, simply made up of people). Systems and policies should be designed in a way that accounts for inevitable mistakes or errors, minimising levels of harm. Second is its multidisciplinary approach, recognising that many factors contribute to improved safety and risk reduction. Behaviours, technologies, architectures, and policies – among many factors – all contribute to cyber security. Effective mechanisms that ensure an integrated approach to these issues is essential.

Recommendation 1: Consider designing a world-first 'Safe System' approach for cyber security.

Language Matters

Dr. Ian Levy, then-technical director of the UK's National Cyber Security Centre (NCSC) and now Distinguished Engineer at Amazon, said in 2016 that "The biggest future threat we have is to keep talking about cyber security the way we do today." The comment was directed at the alarmist rhetoric surrounding the issue. Similar sentiments were shared by Mike Burgess, when he was Chief Information Security Officer at Telstra, in 2015. Speaking about the issue of "threat distraction…Cybercrime is just a crime, cyber espionage is just espionage, hacktivism is just protest", Mr. Burgess noted that for most breaches, the root cause was an issue for which there was a known remedy. He instead called for an emphasis on managing risk and focusing on hygiene.

We see these patterns repeated today. Looking ahead to 2030, our concern is that the rhetoric surrounding cybersecurity will discourage entities from undergoing digital transformation programs, leaving them without the security and performance benefits of modern technologies and with ongoing heightened security risks inherent in many older technologies. Language surrounding sophisticated cyber-attacks may leave smaller entities and individuals with an overwhelming sense of helplessness and confusion at their prospects for managing cyber risks. This needs to change. Industry shares responsibility for shifting away from alarmist and overly technical rhetoric to help small entities and individuals feel empowered to manage their cyber risks effectively. AWS sees an important role for Government in leading this change. By choosing to use non-alarmist, least-technical language, we see an opportunity to make cybersecurity more accessible, achievable, and empowering across the Australian economy and society more broadly.

Recommendation 2: Consciously simplify the language around cybersecurity to make it more accessible, achievable, and empowering.

Focus on Fundamentals

When, in the past, software changes were slow and infrequent, it made sense to bring security in at the end of the development process. As entities move to rapid and agile operating models, this traditional security approach has become cumbersome, earning security teams the reputation of "the Department of No." Security leaders are working to change this perception, by making security support, and even accelerate, the speed and innovation needs of organisations. Incorporating security as a 'business as usual' activity allows organisations and people to innovate safely.

Secure by Design

In a final post on the NCSC's website in late 2022, Dr. Levy reflected on the state of cybersecurity using another unusual analogy – the instrument panel of a B-17 bomber in World War II. While many of these bombers were lost in combat, a great many were also lost during landing. Multiple theories, mostly blaming pilot error, were put forward as the rationale, but it wasn't until after the war that anyone researched the root cause. As it turned out, the switches for the landing gears (which allowed for safe landing) and wing flaps (which did not) were right next to each other – and identical. It was a uniquely tragic example of "blaming users for not being able to operate a terrible

design safely", and resulted in lasting change. Future designs for all aircraft made sure the landing gears and wing flaps were far from each other, and looked distinctly different.

Along those lines, the NCSC has adopted the mindset that "Security that doesn't work for people, doesn't work." The pace of digitisation is not going to slow down, making security by design – in a way that accounts for the humanity at the heart of the security experience – a key feature of future success. This is why security is at the heart of everything we do at AWS, and why security is one of the five pillars of our Well Architected Framework (WAF). The security pillar encompasses the ability to protect data, systems, and assets using design principles that we've identified as best practice for securing workloads in the cloud, but are also applicable more broadly.

Security needs to be as agile as the world it is trying to protect. In terms of policy levers available to government, mandating a set of controls or specifying a framework is not what we recommend; in fact, being overly prescriptive is what we strongly advise against. The real strength of our WAF is that it is principles-based. Technology is not static – we operate in a dynamic security environment that needs to constantly adapt to new technologies, new designs, and new ways of working. Laying out clear, actionable principles for what it means to be secure-by-design in different contexts is one step government can take to supporting the whole of the Australian economy.

Recommendation 3: Government co-creates and publishes secure-by-design principles with industry that takes a flexible and user-centric approach.

Identity is Key

In speaking about the importance of identity to security practices now and into the future, it's necessary to recognise the two dimensions to the issue. On the one hand, there is the macro interpretation of digital identity. This is the dimension of identity that relates to basic human rights, as recognised by the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights: Everyone has the right to be recognised as a person before the law. Everyday activities hinge on people being able to prove their identities and, as governments and private companies around the world digitise, individuals are required to not only prove their identities but to do so via digital channels. To obtain basic services, individuals are often required to provide static forms of identification to a provider, who may then be required to hold that information. This information is then a risk for data theft, most frequently brought about by stolen credentials. And there we find the second, 'micro' dimension of identity: identity and access management.

These are separate but intertwined and intractable issues, both boiling down to the same fundamental requirements: authentication (is the person who they say they are?) and authorisation (does that person have rights of access?). Public digital identity systems, underpinning the provision of legal identity to the population, can address both challenges, granting legal identities to use online. Still, implementing digital ID poses challenges related to data privacy and trust, security, and inclusion. Poorly designed digital ID systems can place

personal data at risk and attract cyber-based threats, necessitating a strong technical architecture and information security framework. We believe that those challenges can and must be overcome through effective implementation, and welcome the announcement following the February meeting of the Digital and Data Ministers of shared intent between the states, territories, and Commonwealth to strengthen Australia's digital identity framework.

Recommendation 4: Government conducts deep consultations on the development of a robust digital ID framework based on foundational and infrastructural models, as a matter of priority.

At the 'micro' level, the importance of identity is something AWS fundamentally understands, and forms the first of our seven design principles for security. As of mid-2022, AWS Identity and Access Management serviced half a billion requests per second. We do this through centralised identity management that eliminates the need for long-term static credentials; that is, we verify cryptographically that the requests are actually coming from who they claim to come from. But we also recognise the human dimension. Although cryptographic authentication is our norm, the human factor – via a vulnerable password – remains. Human failing still needs to be integrated into the approach.

Although we normally caution against prescriptive advice, there is an exception to every rule. Multi-factor authentication (MFA) is one of the simplest and most important protections available to users, making them less susceptible to password leaks or social engineering – which is why we offer free MFA to our customers. Looking over the horizon, we expect that MFA will become fully normalised as a core component of practical cybersecurity, but government can play an important role in speeding up this process. Although MFA is one of the Top Four strategies in the ACSC's Information Security Manual, there is a compelling case for it to be regarded as the most essential. In the US, MFA is being pushed as a baseline online protection by entities such as the FIDO Alliance, NIST, and the US government, which recently issued a statement urging all companies to adopt MFA. The US government, specifically the Cybersecurity & Infrastructure Security Agency (CISA), has taken further measures to drive MFA awareness and adoption by launching the #MoreThanAPassword campaign. We suggest a similar emphasis as part of the new Strategy.

Recommendation 5: Government emphasise and promote MFA as a 'one essential activity' for organisations and users.

Data Governance and Protection

Consistent with our previous submission on the Attorney-General's Department's *Privacy Act Review – Discussion Paper*, we believe the most successful data protection frameworks are those that take a risk-based approach allowing organisations the flexibility to determine the most appropriate measures to manage security risks. Data governance and management policies are important mechanisms to facilitate the provision of clear mandates for data sharing and help reassure data subjects of the security of data collection, use, and storage. AWS sees an important opportunity for the Australian Government to address a genuine policy gap through a clearly articulated approach to data governance and data management. In general, government could

develop a roadmap including broad considerations and guidance for (a) data classification; (b) types of security controls (e.g. IAM, encryption etc.); and (c) organisational controls.

Recommendation 6: Government partner with industry and academia to develop best practice guidance for data governance and management as part of a holistic approach to data protection.

Supporting Small and Medium Businesses

AWS sees an important opportunity for the new Strategy to provide clear messaging and support needed for small and medium businesses (SMBs) to boost their cybersecurity while also maximising the advantages of digitisation. In its 2016 cyber security strategy, the NCSC made a deliberate effort to avoid alarmist rhetoric and put in place consistent, actionable guidance in a single resource. By contrast, while there is an abundance of cybersecurity information available via Australian federal and state government websites, this information is spread across multiple departments and is inconsistent in style and substance. This is reflected in the ACSC's own research: in a study commissioned by the ACSC and released in August 2020, only 36% of respondents were aware of and knew something about Scam Watch. The ACSC had a similarly low awareness rate at 31% of respondents. The level of awareness for Stay Smart Online was even lower, at just 18%.

With the ACSC study also finding that there is a significant unmet demand for more information about cybersecurity, simplifying and consolidating cybersecurity messaging for SMBs is a substantial and meaningful contribution Government can make to improving Australia's cybersecurity. While we have previously welcomed the Government's suggestion of a program in the vein of the UK's Cyber Essentials certification scheme, we again caution against the introduction of new programs before existing initiatives have been properly implemented or assessed. Even with the success of Cyber Essentials, which has been in place since 2014, knowledge of Cyber Essentials as of 2020 among micro and small firms was just 10% and 23% respectively (compared to 40% for medium and large firms). On the basis of ongoing research and surveys to the effectiveness of the scheme, changes have been incrementally introduced over time.

We encourage the Australian Government to similarly take a long-term, evidence-based view to maximising the impact of its support programs. Multiple initiatives intended to support SMBs have been launched over the last two years, including the Cyber Security Assessment Tool and Cyber Security Business Connect and Protect Program, with little ongoing promotion or support to improve the uptake of these initiatives. Uplifting the cybersecurity of SMBs requires real, ongoing commitments over months, if not years. However, this is not the sole purview of government. We think it is a reasonable expectation that larger companies play their part to improve security across the digital ecosystem. AWS is committed to supporting our customers, large and small, with their security. We understand the complexity our customers are facing, and we're determined to simplify cybersecurity to make it achievable, accessible, and scalable. We would be proud to support government in creating actionable guidance for SMBs on safe digitisation.

Recommendation 7: Government conduct an audit of existing programs intended for SMBs, and consolidate the initiatives into a program modelled on the UK's Cyber Essentials.

Strengthening Australia's Ecosystem

Looking ahead to 2030, we see an urgent need for substantial changes in our mental models around cybersecurity. How we build a thriving, resilient, and secure digital ecosystem is one of Australia's most pressing societal and economic challenges. We can rise to that challenge. While the following recommendations are not a 'quick fix' to our current security challenges, they are essential for creating the cultural gear shift necessary for cybersecurity over the longer term.

Mind the (Skills) Gap

Closing the security workforce gap is a crucial step to improving security everywhere. As of 2021, there were 4.19 million cybersecurity professionals worldwide, with a need for 2.72 million more. While security professionals keep joining the workforce, the need for security professionals outpaces the supply. Some ways organisations can help close the security workforce gap are to invest in diversity, equity, and inclusion initiatives, reevaluate hiring standards and practices, and invest in candidates with diverse backgrounds. We believe organisations will be more secure and successful if they hire for attitude and aptitude, and train for technical skills. Organisations should look beyond specific technical degrees and certifications and instead try to hire people who have the aptitude or skills in other forms.

Diversity in security is about more than equality; it is about optimising defensive capabilities by having access to the widest possible range of problem-solving abilities. Consider that around half of security professionals got their start outside of IT; we think this is a strength for the sector and should be encouraged. But recent research conducted by RMIT is a sobering reminder of how much more there is to do. RMIT's March 2023 study on women in cybersecurity revealed that, as of the 2021 Census, women comprised just 17% of cybersecurity occupations[1]. Of the women in the field, around half have a degree in a field other than IT. This disparity is based in deep historical and societal trends, and requires focused, generational shifts.

Of course, diversity is about more than gender. For example, organizations such as GCHQ, the UK's signals intelligence agency, are leading the way by actively hiring neurodiverse individuals for their unique ability to spot patterns in data. Creating workplaces that not only welcome, but celebrate and understand the value of diversity, requires ongoing and systemic cultural change. We need to encourage this change through the development of future staff through mentorship programs, and by connecting with the future generations of the workforce.

While addressing the cybersecurity skills gap is important, we also believe that having a cybersecurity literate society and broader workforce is equally important for reducing risks over time. The need for a cybersecurity literate workforce is reinforced by findings from a report

[1] For the purposes of this report, we are using gender terminology as adopted by the RMIT report based on Census data. However, we also acknowledge individuals who identify as non-binary, gender fluid, and gender diverse.

commissioned by AWS and prepared by AlphaBeta, which found that 64% of Australian workers already apply digital skills in their jobs. Industry can play a part in meeting this need. At AWS, we are already making significant investments to make it easier for people to gain the skills they need to grow their careers in cloud computing, including cybersecurity. We've trained more than 300,000 people across Australia with cloud skills since 2017, and support programs like Grok Academy and the Tech Girls Movement Foundation. We would happily support government initiatives in expanding the accessibility of these skilling and 'cybersecurity literacy' programs.

Recommendation 8: Government partner with industry to create a national mentor program in cybersecurity.

Recommendation 9: Cybersecurity education and training should be integrated into school curriculums and non-cybersecurity university and TAFE programs.

Embrace Automation

While security primarily requires a human-focused effort, automation can and will play an increasingly important role across the digital ecosystem. Historically, security has been a binary, rules-based system in which things are either okay or not okay. Modern technologies, including cloud, have disrupted this binary. Instead of building complex systems that define "okay" based on a number of criteria, we can now dynamically build strong defences and effective hedging strategies against known threats. Automation is also rapidly emerging as essential to effective cybersecurity operations. Right now, for example, well-equipped security teams make use of automation to reduce 'noise' in their alerts and incident response.

While many of the use cases for automation are still reactive, this is rapidly shifting, particularly in cloud environments. Predictive capabilities derived from collected information can play a significant role in making cybersecurity more proactive by identifying outliers and offering recommendations about how to address vulnerabilities. Moving forward, instead of conducting periodic cybersecurity reviews, we see a future where organisations shift to continuous automated cybersecurity assurance. We also anticipate that machine learning will play a major role in augmenting security engineers' capabilities, helping them to create more secure architectures and applications. For example, it will simplify the automation of cybersecurity tasks such as patching, logging, monitoring, auditing, and integration with existing toolsets.

The possibilities are substantial, and real. Automation will help create an environment where it's easier to make the best cybersecurity decisions earlier in the development of business processes and digital products. Cybersecurity will be truly built into everything organisations do, which is the right approach. Modern technologies provide an exciting opportunity to help drive this, and to secure data in ways that weren't previously possible. This, however, depends on major modernisation efforts.

Recommendation 10: Government encourage and support the development and use of automation technologies for the purpose of cybersecurity improvements.

Keep Left and Modernise

Some of the most important cybersecurity advances any organisation can make are not necessarily security-related. As technologies continue to evolve and digitisation accelerates, cybersecurity investments will necessarily need to become more dynamic and integrated into all business decisions. Effectively integrating cybersecurity into all business decisions will take time – and, in many cases, will necessitate a rethink of well-worn investment processes. But failing to accelerate the transition away from legacy IT systems, and legacy business processes, leaves many Australian entities at risk. We encourage the Australian Government to partner with industry, academia and professional associations to develop a risk and resilience culture that encourages, rather than inhibits, innovation and digitisation.

Modernisation is needed. For many entities, IT management cycles are rooted in outdated practices – annual capital and operational expenditure cycles; in-house charging models emphasising lowest cost of delivery; outsourced operations that leave workers with little or no incentive or opportunity to upskill; and rigid deployment cycles that leave no opportunity to iterate and 'build in' security or address risks as they arise. Because systems in this model are viewed as projects, rather than long services, the investment cycle oscillates from 'deploy' to 'run', leaving those systems without ongoing funding beyond sustainment. Many entities are then forced to continue running outdated systems, sometimes long after the system has aged out of support from the supplier, with no means of upgrades or replacements without the allocation of additional capital funding.

As technologies continue to evolve and digitisation accelerates, cybersecurity investments will necessarily need to become more dynamic and integrated into all business decisions. A new model is necessary to achieve this integration. Without understanding the priorities of an organisation, its business model, or its culture, it is not possible to effectively manage any business risks, much less cyber-risks. Traditional 'plan, build, run' IT operations and funding models are ineffective in creating the continuous feedback and improvement loops necessary for operational excellence and, as a result, these old methods prevent any substantial security improvements. We would welcome the opportunity to dive deeper on this important issue with government, which would have significant economic and cybersecurity benefits.

Recommendation 11: Government partner with industry, academia and professional associations to develop guidance that helps boards and senior executives understand how to incorporate cyber risks into investment cycles.

Recommendation 12: Government partner with industry, academia and professional associations to develop a new, fit-for-purpose funding model for digital infrastructure and software investments.

Regulatory Simplification

Government has an important role to play in creating a cybersafe ecosystem through regulatory measures, the creation of incentives, building awareness across the whole of society, and providing guidance. As articulated earlier in our submission, we also see an urgent need for investment and risk management approaches that encourage, rather than inhibit, innovation and digitisation. Achieving these outcomes requires consistency and clarity, balanced with necessary flexibility. We agree with the Office of Best Practice Regulation that the introduction of new regulations should not be the default, but see clear opportunities to improve Australia's legislative and regulatory frameworks around cybersecurity, privacy, and data protection.

Toward a Single Federal Framework

To ensure consistency, avoid confusion and maintain a common language and understanding of cybersecurity, privacy and data protection expectations, a harmonisation and simplification of the regulatory environment would be beneficial to both business and government. In her foreword to the Discussion Paper, Minister O'Neil posits that "Australia has a patchwork of policies, laws and frameworks that are not keeping up with the challenges presented by the digital age". We agree. There are at least 51 Commonwealth, state, and territory laws that create, or could create, some form of cybersecurity, privacy or data protection obligation. Consequently, the risk of confusion, conflicting or overlapping regulations is high. A 2018 study by the MITRE Corporation, commissioned by AustCyber, found:

> [T]he abundance of standards and guidelines available to Australian organizations at both the federal and state/territory level caused confusion around what advice should be adopted. "Cyberaware" organizations are overregulating, doing nothing, or applying a mixture of domestic and international standards for guidelines. The result is inefficient and is a barrier to improving Australia's cyber resilience. The Australian government can begin to address this issue by taking steps to harmonize the guidelines it provides to industry and other levels of Australian government.

Five years later, this assessment stands. Simplification and consolidation of cybersecurity regulations and messaging should be an important element of the Australian Government's ongoing efforts to support cybersecurity across the Australian economy and society. In careful, considered consultation with the states and territories, we suggest the creation of a federal legislative model for cybersecurity, privacy and data protection, bringing the Commonwealth, states, and territories under a single regulatory umbrella. By necessity, this single framework would involve integration with state and territory incident response, notification, emergency, and crisis management mechanisms. Importantly, it also does not involve immediately creating new obligations and would instead allow for a proper assessment of current legislative and regulatory obligations. While this is a complex and ambitious suggestion, we consider it is achievable and beneficial for Australia's longer-term cybersecurity successes.

Recommendation 13: Allow time to implement and assess recent, ongoing or existing legislative and regulatory reforms, frameworks and programs before significantly changing those measures or introducing additional regulatory measures or compliance programs.

Recommendation 14: The existing legislative and regulatory environment applicable to cybersecurity, privacy and data protection should be simplified and harmonised into a single federal framework.

Recommendation 15: Any new obligations or regulatory measures should be principles-based to give entities necessary flexibility to appropriately manage their unique circumstances and security risks, and to ensure that these changes are future-proofed as much as possible.

Establish Technical Grounding

One of the tenets of this paper is to ensure that policies, guidance and frameworks are fit-for-purpose and reflect the realities and benefits of technologies. We believe it is essential that there is a dedicated, independent statutory authority with the focus and necessary technical expertise to oversee Australia's cybersecurity framework as government continues to grapple with the policy challenges posed by technological change, particularly on the question of technical feasibility. A Technical Advisory Committee, loosely modelled on the ACMA Authority and made up of academia and industry experts, could be one possible means of achieving this technical grounding. We also see this kind of mechanism as important for building and maintaining trust with industry, enabling the contestability currently lacking in important areas of policy that impact, but are not directly related to, cybersecurity – for instance, electronic surveillance reforms, critical infrastructure, and critical and emerging technologies.

Recommendation 16: Government consider the creation of a Technical Advisory Committee for cybersecurity and adjacent areas of policy.

Educating Boards and Senior Executives

As expressed in our response to the *Strengthening Australia's cyber security regulations and incentives* discussion paper, AWS supports the creation of guidance to help boards in understanding how to engage with cybersecurity risks, rather than imposing new and highly specific obligations on directors. At its core, cybersecurity is a business risk, and is already part of a director's existing duties. This was acknowledged by the Australian Securities and Investments Commission (ASIC) in 2015's *Report 429: Cyber Resilience*, which clearly articulated that Australian directors are responsible for building and maintaining cyber resilience and offered guidance on resilience practices. In the same report, ASIC also acknowledged that many regulated entities already had proactive and sophisticated risk management practices to address cyber risks – but that even then, it was not possible to protect against all cyber risks:

> As cyber attacks continue to increase in complexity and sophistication, invariably you may be subject to an attack. However, you can seek to improve your overall cyber resilience so you can survive and recover from an attack as quickly as possible.

A voluntary code may assist directors in making more informed investment decisions, but we caution against overly prescriptive codes that emphasise compliance with prescriptive technical controls at the expense of a holistic risk management strategy. Any guidance should be principles-based and recognise that each organisation's risks, priorities, and systems are unique. Integrating cybersecurity into all business decisions will take time and, in many cases, will necessitate a rethink of well-worn investment processes. Industry, academia and professional associations are well-placed to partner with government for the development of practical, risk-based cybersecurity guidance and outreach programs for boards and senior executives that assists in making those long-term investment decisions. We encourage the Australian Government to partner with industry, academia and professional associations to develop a risk and resilience culture within Australia's boards that also encourages, rather than inhibits, innovation and digitisation.

Recommendation 17: Government should partner with industry, academia and professional associations to develop guidance that helps boards and senior executives understand how to manage cyber risks and their obligations and responsibilities.

Incident Reporting and Response

AWS supports the concept of a single reporting portal for all cyber incidents and notifiable data breaches to harmonise existing requirements to report separately to multiple regulators. Going a step further, we recommend a consolidation of other reporting requirements related to security, including reporting of owner-operator and asset information under multiple regulatory mechanisms (e.g., the Hosting Certification Framework, foreign investment laws, and critical infrastructure laws, which all require entities to provide similar sensitive information via multiple channels). The existing requirements create substantial regulatory duplication for reporting entities, and mean that sensitive information is widely dispersed, creating its own potential security risks. However, we do not support expanding the existing notification regime for cybersecurity incidents. The current obligations require time to mature and fully implement, and government should focus on assessing the value derived from current incident reporting before expanding the regime.

Recommendation 18: Government consolidate cyber incident reporting into a single portal, and should consider consolidating reporting requirements for other security-related regulatory regimes.

Recommendation 19: Government does not expand existing incident reporting obligations until existing measures have been allowed more time to mature and be fully implemented, and their value has been fully assessed.

Purposeful Partnerships

Cybersecurity is a collective challenge, and AWS is committed to collaborating closely with government. We see tremendous value in creating and maintaining genuine partnerships between government, industry, and academia to achieve shared strategic objectives. Through existing

mechanisms such as the Trusted Information Sharing Network (TISN), government can leverage the expertise, experience, and reach of large enterprises to promote and support strong national cybersecurity outcomes. But true collaboration can only follow from shared strategic purpose, intent, and commitment. Existing initiatives, such as the Joint Cyber Security Centres, have not seen their potential fulfilled, at least in part because 'collaboration' is not an objective – it is the means of achieving an objective.

Strategic Objectives, Shared Intent

We strongly encourage the new Strategy to consider existing forums – particularly the TISN – as a means of developing shared objectives between government and industry to meet common challenges. In the last year, since the standing up of the Data Sector Group, we have seen significant value in the TISN as a means of creating trusted, productive partnerships with government in pursuit of common goals. Just as importantly, it provides a forum for open and robust conversations on contentious issues, allowing for a full exploration of the complexities of the subject matter at hand. This should not only be welcomed more broadly in conversations around cybersecurity, but actively encouraged.

We also welcome Minister O'Neil's recent announcement that the new National Cyber Security Coordinator will be leading a regime of cyber exercises, and see real potential for the Coordinator and supporting Office to play a central role in facilitating ongoing and purposeful engagement with industry. It is vitally important that, for the purposes of meeting the ambitions of the new Strategy, consultation and engagement does not stop with the submission of consultation papers. AWS looks forward to engaging with the Coordinator and their Office on pathways for improving Australia's cyber resilience.

Recommendation 20: The Strategy considers how to fully utilise the TISN as a mechanism for outcome-driven industry engagement.

Recommendation 21: The new National Cyber Security Coordinator and their Office play a substantial role in facilitating ongoing and purposeful engagement with industry to define and address strategic cybersecurity objectives.

Threat Sharing and Blocking

Cybersecurity requires continuous assessments and reviews of threat activities; as technologies and threat activities evolve, so must cybersecurity as a practice. Maintaining situational awareness is important for creating resilience across the entire Australian ecosystem, and some entities, including AWS, invest heavily in their threat intelligence and cyber capabilities. But we come back to core points from earlier in our submission: many entities are simply caught in a cycle of attempting to address the 'tech debts' of legacy IT infrastructure. Fundamentals, such as security by design and data governance, are not yet in place. Many entities do not have the internal integrations necessary to make use of technical threat intelligence, and for smaller entities, they may have no capacity – or the means of acquiring the capacity – to implement threat detection

and blocking regimes at all. Threat intelligence is important, but it is not a silver bullet to addressing these baseline issues and should be shared or received on a voluntary basis.

One complementary activity to the distribution of threat indicators would be the creation of a secure data lake by government. This would allow entities to interrogate and draw on available indicators for the purposes of threat research and discovery. Entities could also choose to anonymously share anonymised information from their own environments into the platform (after the information was subject to a process of normalisation and validation) – again, on a voluntary basis. Referring back to our previous recommendations around strategic objectives, this type of resource could be used as the basis for collaborative investigations or hypothesis testing – allowing for a more proactive use of intelligence, rather than passive ingestion methods. It would also allow for targeted analytical activities designed, for example, to support a particular sector or target a particular type of crime. On the basis of this analysis, evidence-based guidance could be developed.

Similarly, the design of any threat blocking regime is something that requires extensive consultation and must have strong technical grounding. This is something AWS fundamentally understands, and we are happy to share more detailed thoughts on best practices; through our integrated and automated capabilities, such as GuardDuty and Lambda, we continuously monitor for threat activity and initiate automated isolation, investigation, and remediation actions. Our internal DNS, Route 53, allows users to securely connect to their AWS services and provides additional blocking capabilities through the Resolver DNS Firewall. Importantly, our architectures allow for sandboxing – where we are able to query unfiltered information to derive further intelligence on threat activities – and customisation, to prevent the inadvertent blocking of legitimate traffic. We would welcome the opportunity to workshop a holistic approach to threat treatment with Government as part of the development of the Strategy.

Recommendation 22: Government create a secure data lake of threat information, allowing entities to directly query and, if they choose, share anonymised information to the platform.

Recommendation 23: Government works with industry to develop a program relating to 'threat treatment' that assesses blocking capacity, but also considers isolation, investigation, and remediation actions within risk tolerances.

The International Dimension

As the issues paper recognises, improving Australia's cybersecurity does not happen in a domestic vacuum. There is an opportunity for Australia to leverage its position as a trusted global voice on cyber security, including by continuing to promote international rules and norms and working with regional partners to build cyber resilience. AWS welcomes the opportunity to support the Australian Government's objectives in this space and would be happy to support the Government in developing an updated international cyber engagement strategy and action plan. While it is useful to have an international dimension included in the new Strategy to ensure strategic

alignment, we believe it would be helpful to have a separate mechanism for international engagement to maintain momentum and focus in this space.

Recommendation 24: Government initiates a separate consultation for the foreign policy elements of the Strategy.

Regional Cyber Resilience

Many of our recommendations for building cyber resilience in Australia are applicable for building Pacific resilience, particularly relating to foundational infrastructure as the prerequisite for more advanced cybersecurity capabilities. AWS would be pleased to engage on a plan for building that foundational capacity. We see scope for government to better integrate industry into key conversations with regional partners to help improve regional cyber resilience, including opportunities to collaborate on capacity building programs. Importantly, these efforts should recognise the particular needs of different geographies; while cybersecurity is one important element of resilience, there are many others (for example, we are acutely aware of the connectivity and digital resilience considerations of severe weather events).

Recommendation 25: As part of a regional resilience plan, Government prioritise broader foundational capacity building and take a holistic view of resilience to disruptive events.

Global Rules, Norms, and Standards

Australia has played an important role in working with likeminded partners to shape international rules and norms in cyberspace, following on from the 2021 International Cyber and Critical Tech Engagement Strategy. It would be helpful for Government to articulate how it plans to build on this work in the period leading to 2030 and work with industry to identify opportunities for collaboration. This needs to be approached from a position of trust and industry partners should be brought into the tent to ensure alignment with Government objectives. For example, there is scope for greater collaboration on international cyber and tech standards. AWS recommends that Government develop a set of priorities (and priority standards forums) for cyber and tech standards and work in partnership with industry and academia to develop a targeted action plan for engagement. A mechanism for ongoing collaboration should also be established, which would include government, industry and academic experts and practitioners. This could form part of the existing work program under the Quad Standards Working Group in the first instance.

Recommendation 26: Government work with industry and academia to develop a set of priorities for cyber and tech standards, followed by an action plan for ongoing engagement.

A Simplified International Framework

In the spirit of simplifying and reducing complexity, we recommend that Government work with likeminded partners and Governments to identify mechanisms for enhancing cybersecurity while reducing duplication across jurisdictions. This complexity results in multinational entities needing to demonstrate compliance with similar frameworks in separate geographies, each with marginally different requirements that accumulate to significant regulatory burdens and duplicated efforts.

It is also an inhibitor to Australian entities – especially tech companies – being able to easily pursue overseas opportunities. A mutual recognition program would substantially reduce that duplication, and provide an opening for Australian entities internationally. In the first instance, we suggest hosting frameworks as a candidate for this type of engagement, focusing on AUKUS as a key partnership. Part of this process would require a comparative assessment between the three countries, and working to bring hosting frameworks into direct alignment.

Recommendation 27: Government work to establish an AUKUS Mutual Recognition Scheme for government hosting frameworks.

Intersection with Critical and Emerging Technologies

Future proofing is an important consideration for a new Strategy. Enabling Australia to achieve the Government's goal of becoming the 'most cyber secure nation by 2030' requires a vision for Australia and Australians will engage with emerging and critical technologies now and into the future, and how these technologies will interact with Australia's cyber resilience. Technologies such as AI/ML and quantum have the potential to significantly transform society and, of course, in many ways already are. The potential for quantum technologies to disrupt existing encryption systems is significant, and one example for why the Strategy should include a plan for how organisations can start thinking about the future security implications of emerging and future technologies.

While much of the discussion around the development of the Cyber Security Strategy has considered how existing technologies, such as automation, can help simplify cyber hygiene, the issues paper doesn't currently articulate how the Strategy will interact with a rapidly evolving technology ecosystem. We have tried to address this issue in our recommendations on security by design and establishing clear principles, but the success of those recommendations will depend on their integration with other relevant policy programs (such as the imminent National Quantum Strategy and List of Critical Technologies in the National Interest). Understanding the technologies of strategic significance to Australia, and the opportunities and risks they represent, is an important step in securing our future national prosperity and stability. Cybersecurity should be incorporated as a key consideration, in line with a systems-thinking approach.

As we articulated in our response to the *2022 List of Critical Technologies in the National Interest* consultation, we recommendation that the Strategy consider the technology lifecycle for continuous assurance, starting with the principle of secure by design. For instance, established, institutionalised and optimised technologies may require ongoing security assurance, whether via regulation or standardisation, as their application evolves – particularly when those technologies are also considered critical infrastructure. Emerging technologies, on the other hand, may not require such immediate interventions, but would benefit from guidance on secure by design activities for their early stages of innovation and development. As a technology becomes more established, those assurance requirements may necessarily evolve. Technology readiness levels or

other maturity mapping approaches could be applied to Technology Profiles for lifecycle assurance considerations, from research and development, to deployment and retirement.

Recommendation 28: The Strategy clearly articulates interactions with other key areas of tech policy, such as the Critical Technologies List, and links key concepts such as secure by design and continuous assurance to these policy programs.

Conclusion

The complexity and scale of the cybersecurity challenge demands a clear, cohesive, and comprehensive approach that simplifies cybersecurity and increases the ease and success of implementation. How we evaluate the success of the new Strategy will depend on the approach chosen. Coming back to our suggestion of adopting a Cyber Safe System, we can open a range of possibilities for measuring success beyond simple metrics around numbers of reported incidents. This holistic approach would allow government to evaluate the complexities of how and why a cybersecurity incident was able to take place – not just at or from the point of compromise, but 'tracking back' through direct and incidental causal factors that lead to the circumstances of compromise.

Just like road safety, people are at the heart of cybersecurity. As described by the architects of Vision Zero, "In every situation a person might fail. The road system should not." This changes the formulation of how we think about road safety. Instead of expecting people to adapt to an imperfect system, we design the system for people. Cybersecurity can and should take a similar approach. While we have delivered a breadth of recommendations, they are all grounded in the tenets outlined in our introduction and based in a belief that a systems approach is necessary for meeting this challenge.