AUCLOUD

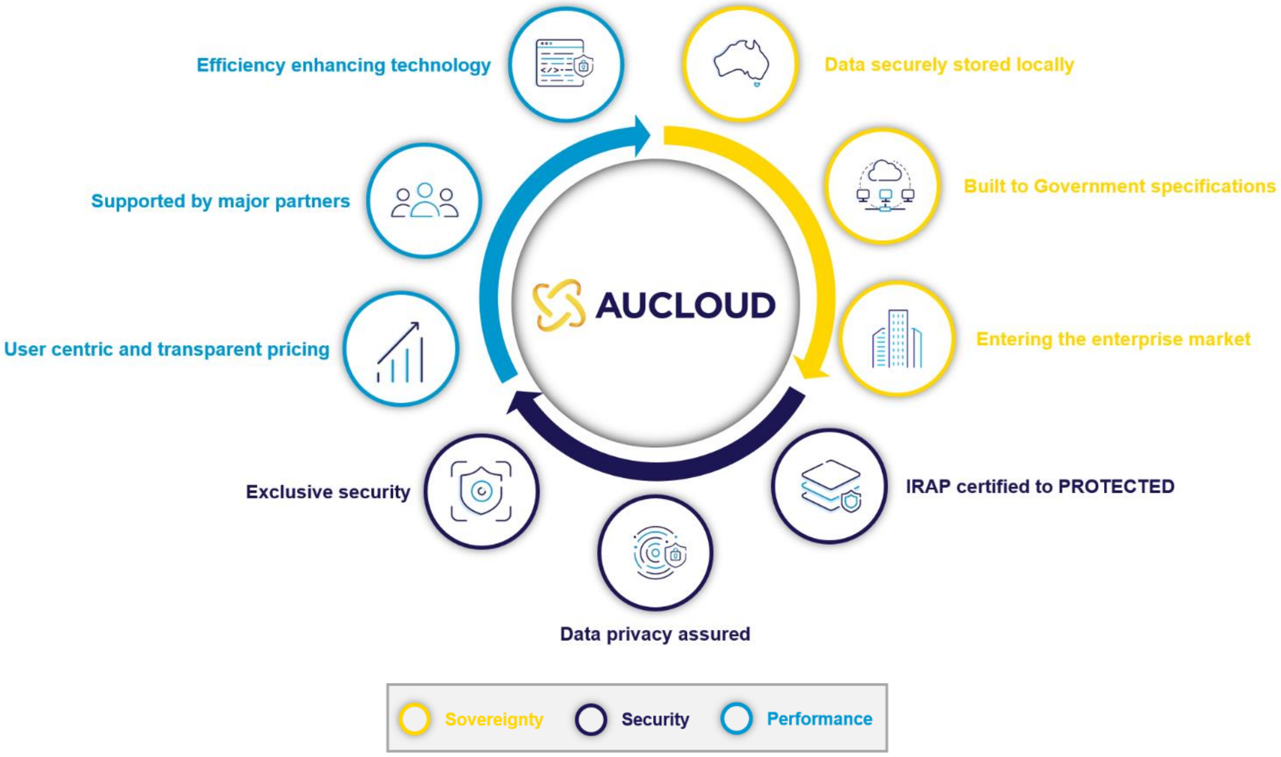
Cyber Security Strategy 2023-2030

AUCloud Response to Discussion Paper

APRIL 2023

About AUCloud

Sovereign Cloud Australia Limited, trading as 'AUCloud', in an Australian sovereign cloud and cyber security services provider. Established in 2017 and listing on the Australian Stock Exchange (ASX) in December 2020, AUCloud have a footprint of six platforms across Canberra, Sydney, Brisbane and Melbourne with all services Information Security Registered Assessors Program (IRAP) assessed to meet the 'Protected' controls of the Information Security Manual (ISM).


Efficiency enhancing technology
Data securely stored locally
Supported by major partners
Built to Government specifications
AUCLOUD
User centric and transparent pricing
Entering the enterprise market
Exclusive security
IRAP certified to PROTECTED
Data privacy assured
Sovereignty
Security
Performance

Our cloud solutions and cyber security services support and are trusted by a wide range of industry leaders, including:

- **Global Systems integrators** like DXC to provide high availability, resilient compute, storage and back-up infrastructure for e-health records for the Australian Defence Force.
- **Direct Government agencies** like the Australian Electoral Commission (AEC), where we provided our Security Operations Centre (SOC) and Cyber Threat Monitoring Services to support and, to quote their CISO, "help defend democracy" of the Federal Election along with the election integrity task force including Home Affairs.
- **A wide range of companies in the cyber security, software and services space**, (e.g. Fifth Domain who use software code to spin up thousands of compute instances during the period where the national CSIRO Cyber Taipan event or Australian Defence Force (ADF) cyber training competitions take place.)

Overview

Sovereign Cloud Australia Pty Ltd (ASX: SOV) (trading as AUCloud) welcomes the release of the Cyber Security Strategy 2023-2030 Discussion Paper and the opportunity to provide views on how all organisations and citizens can work collectively to achieve the vision to make Australia the world's most cyber secure country by 2030. We recognise the importance of consultation and collaboration that will inform your recommendations to Government about how we can better protect and enhance our collective cyber resilience, both in Australia and in the region.

As a Certified Strategic[1] sovereign provider of cloud Infrastructure-as-Service (IaaS), where the information assurance considerations of availability, confidentiality and integrity are tightly linked with aspects of data privacy, AUCloud has a proven track record of participation in industry consultation relating to cloud, cyber security and data. Our insight end expertise is based not only on the experience of providing cloud services to a growing customer base of Governments, national critical infrastructure customers and security conscious organisations who collectively delivery systems of national significance but also the experience of Phil Dawson (AUCloud's Founder and Executive Director), who is a member of the Australian Information Industry Association's ACT and Federal Council since 2019. Prior to founding AUCloud, during 2012-14, Mr Dawson co-authored the UK Data Capability Strategy[2] for the UK Minister of State for Universities and Science and Chaired the UK Industry Association's (TechUK) Cloud, Data Analytics and Cyber Security Committee.

AUCloud strongly supports the updated Cyber Security Strategy 2023-2030 to define the priorities for Australia's cyber security and accelerate uplift of Australia's capability to deliver an economic environment that is safe, trusted and secure, within a thriving cyber ecosystem, and supporting resilient and secure Government and critical infrastructure systems.

We welcome the recognition that the strategy must reflect the importance of protecting customer data, ensuring that all organisations have the right cyber security settings in place and that a critical feature for achieving resilience within the stated vision will be for more effective development of Australia's sovereign capability. Capability that will move beyond a niche technical field to a strategic national security capability, ensuring, as we transition to a digital economy, that sovereign control of critical delivery (NCIs) organisations with custodianship of underlying citizen data delivers the essential ongoing trust that our personal data, infrastructure, and underpinning systems are secure.

[1] Digital Transformation Agency Hosting Certification Framework

[2] https://assets.publishing.service.gov.uk/Government/uploads/system/uploads/attachment_data/file/254136/bis-13-1250-strategy-for-uk-data-capability-v4.pdf

AUCloud's core perspective on all matters relating to cyber security and the related area of privacy, is that ultimately it is all about the DATA; the availability, confidentiality and integrity of all data types (customer data, support data, monitoring data, metadata and derived or inferred data from analysis of the other data sets) as these attributes of data are fundamental to system operations, derived insights, consequential actions and overall cyber security vulnerability. This, in our view, drives a criticality to ensure the formation of a common definition and understanding of data for all aspects (cyber security, privacy, procurement, insurance, etc) across all Governments, organisations and for Australians in general.

AUCloud is proud to be a leading member of the growing, vibrant domestic ecosystem of sovereign controlled providers of a wide range of cyber security capabilities. This includes the build and maintenance of the critical underlying infrastructure through to robust cyber security software solutions and a wholistic range of supporting services. All of which are designed and motivated by contributing to the development of stronger domestic cyber security capability and posture through identifying, training and nurturing Australian cyber security talent across the country.

For Australia to establish the desired national cyber resilience and sovereign capability by 2030 investment and focus by the Australian Governments needs to be on procuring services locally. Australian-born sovereign providers are at the forefront of innovation, are accredited and rigorously governed, practice and help define global best practice and have a proven track record of supporting a significant element of Government and National Critical Industries. Procuring from Australian made cyber security and sovereign cloud providers is the single most rapid and effective avenue to develop an enduring and adaptive sovereign capability, whilst helping build local skills and expertise required to maintain the cyber resilience and posture Australia requires by 2030 and beyond.

Current providers are Australian controlled and headquartered companies that are already known and working in partnership with allies (AUKUS, 5EYES) and regional neighbours to lift cyber security, counter cyber threats and build a cyber resilient region.

We look forward to participating in this and on-going discussions to improve Australia's cyber security capability and ultimately deliver sovereign resilience for the benefit of all citizens

- through understanding the importance of data and the constituent elements,
- through consideration of the role that an enhanced domestic eco-system of cyber capability can bring to establish sovereign control and self-determination;
- through the role Government and Government procurement can play to amplify market investment in domestic capability to develop skills, to grow and develop IP and to create a strong exporting ecosystem; and,

- through communication and amplification of existing best practices within country and supporting regional neighbours

Summary

We believe Australia requires a mixed economy of global, national and local technology providers to support and protect all parts of our economy, from our international trade activities through to those activities and operations critical to Australia's democracy, national security and indeed sovereignty.

We believe that successful achievement of the outlined vision will be underpinned through focus on five key areas to cement a strong cyber security foundation, building a resilient cyber workforce and position Australia as a global leader in security:

1. **The importance of 'Defining Data'** - in terms of both security and privacy, there is a fundamental requirement for one common and meaningful definition across both public and private sectors, which aligns cyber security, privacy and procurement's contractual considerations.
2. **Sovereign Resilience** - increased focus on true sovereign resilience, control and governance to protect critical infrastructure, to foster a vibrant domestic ecosystem and in turn to drive Australian intellectual property (IP) and reputation across the global cyber security industry.
3. **Stronger Domestic Capability –** mechanisms and policies to help stimulate, foster and grow a critical workforce for the industry, supporting the domestic economy, security and international partnerships.
4. **Accelerating Best Practice behaviours –** better promotion and enhanced adoption of existing security, assurance and privacy frameworks and behaviours can not only help uplift the cyber capability of Government, critical infrastructure and large enterprises but also secure data and increase resilience of SMEs and individual citizens.
5. **Acting with Pace and Adaptability –** whether in the context of more invasive, broad based, cyber compromise or the adaptation of new technologies, threat actors and the world are not waiting for anyone to catch up or develop policy, therefore a change of pace for hastened improvement and openness to adaption will be essential to success.

Recommendations

The importance of "Defining Data"

Defining data and all associated elements is fundamentally imperative. Defining data is essential from the perspectives of 'confidentiality', 'integrity' and 'availability'. Data is a short word that means many things, to many people; formally and informally defined in numerous ways across Australia. Data is critical to the delivery of world class cyber security and personal privacy for all Australians yet materially there is no consensus on its very definition.

Data, the very thing we are trying to protect, must have a common definition within both the public and private realm. For example, Government currently applies alternative definitions to data across different domains whether 'procurement', 'information security' and 'privacy'. A few current examples of definitions pertaining to data or the abstracted level of information include:

- The National Data Security Action Plan[3] currently defines data as:
  - Data is any information in a form capable of being communicated, analysed or processed (whether by an individual or by computer or other automated means).
  - Data can include personal information, which is information about an individual or an individual who is reasonably identifiable – such as their basic contact details, records generated through their interaction with services or the internet, or information about their biometrics (physical or behavioural characteristics). Data can also include population-level data, such as demographics.
  - Data can include information that can be used to describe location (such as geospatial reference details) or the environment (such as biodiversity or the weather). It can also refer to the information captured or generated by the networks of sensors that make up the Internet of Things.
  - Data about systems can include administrative records about businesses and public services.
- A Government Agency's head agreement for a marketplace/panel procurement defines data as:
  - All data and information (including personal information) generated by or relating to Agency and its functions (including data relating to Agency's operations, assets, programs, personnel, clients and other entities) in whatever form that data and information may exist.

[3] National Data Security Action Plan (homeaffairs.gov.au)

- A commercial organisation's sub-contract definition based on their prime contract working to a Government agency:
    - Contractor data means all information entered on storage media or equipment by or on behalf of Contractor or their respective employees, contractors, agents, Contractors, and End Users, and information derived from such information, including Personally Identifiable Information.
- Recommendation 4.1 within the current review of Privacy legislation suggests amending the definition of Personal Information (PI) to change the word 'about' in the definition of personal information to 'relates to'. Where Section 6 of the Privacy Act currently defines personal information as
    - personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not. The Individual is defined as a 'natural person'.
    - The rationale is that replacing 'about' an individual to 'relates to' would not significantly change the definition, but would make it clearer that technical and inferred information can be personal information (i.e. the metadata relating to the person).

We recognise that each instance cited above has different context and purpose that drives the level of abstraction. However, the lack of clarity as to the underlying elements of data and by implication consideration of the related risks associated with availability, confidentiality and integrity of that data has the potential to remove clarity of purpose and ownership of those risks (i.e. that all data types are prone to confidentiality, integrity and availability compromise that can impact systems and/or provide vectors for future compromise risk).

We believe a stronger and clearer definition that would address this risk is one that was determined by the ACSC within the Cloud Assessment and Authorisation Framework[4], in the context of Cloud Service Providers (CSP), which identified the most common data types as:

- **Customer data**: This is data the Cloud Consumer creates, generates or uploads to the CSP for storing, processing and sharing using the CSP's cloud services, this includes the Cloud Consumer's authentication data. The Cloud Consumer, as the data owner, remains

[4] https://www.cyber.gov.au/sites/default/files/2021-10/PROTECT%20-%20Anatomy%20of%20a%20Cloud%20Assessment%20and%20Authorisation%20%28October%202021%29.pdf

accountable for the security of this data type, including any compromises, losses or damages that occur.

- **Account data**: This is data about the Cloud Consumer’s account with the CSP and can include billing information, contact information and usage information
- **Metadata**: This includes data about the Cloud Consumers’ use of the CSP’s cloud services and can include Cloud Consumer generated information such as resource names, service tag details and utilisation information.
- **Support and administrator data**: This data type is provided to the CSP’s support personnel and administrators for technical support purposes. This can include logs, monitoring alerts and error report information.

A generic version of the ACSC definition would be:

- **Customer data**: This is data created, generated or uploaded by an End User to a service provider for storing, processing and sharing, including any related authentication data.
- **Account data**: This is data about the End User and their account with the service provider and can include billing information, contact information and usage information
- **Metadata**: This includes data about the End User and their use of the services and can include system generated information such as resource names, service tag details and utilisation information.
- **Support and administrator data**: This data type is provided to the service providers support personnel and administrators for technical support purposes. This can include logs, monitoring alerts, error report information and inferred or derived data.

Improving Sovereign Resilience

Government’s main priorities are to make Australians more prosperous and successful, and equally to improve Australia’s security on a global scale. Sovereign capability are critical necessities if either priority is to be achieved, providing resilience and self-determination, with their importance sharply highlighted during recent weather and pandemic type events.

Sovereign capability is the combination of the ‘domestic capability’ to supply a product and/or deliver a service with the ‘sovereign control’ over the assets and skills that underpin the delivery capability. In the cyber security domain, an ecosystem of proven, accredited sovereign capability (providers) already exists, currently delivering a comprehensive range of products and services to a large base of organisations.

When we consider sovereignty of data from a security standpoint we must consider:

- Without access to Australia's data, how do you do we protect Australians and Australia's interests?
- How do we recover if our core data hasn't been backed up within our sphere of legal, territorial or personnel control and the data recovery requires access to overseas services or expertise?
- Access and backing up data are identified within the Essential Eight as a core protection strategy. It is that basic.

A key element to address these questions is about improving Australia's sovereign resilience, enabling self-determination of and requiring sovereign control by Australia. Data itself, across all domains of people, process and technology, is a key element in establishing sovereign capability. This requires not only recognition of the importance to build such capability, combined with the need to effect clear actions to encourage investment to develop homegrown expertise and intellectual property not only for today but for a highly skilled workforce and related industry into the future.

Government has a pivotal role to play in driving and improving sovereign resilience. It is one of the single largest and most credible customers when it comes to data and security in the country, and its influence on encouraging external investment cannot be overstated. Government procuring services from Australian owned companies begets external market investment, which begets a growing and virtuous ecosystem of cyber security capability. Procuring not for any feel good patriotic duty, but because existing going concern Australian companies across the cyber security ecosystem are more than capable of delivering and supporting national scale, high-risk, high-profile services for Government and critical infrastructure in-country, without cause or need for overseas personnel accessing Australian systems. Furthermore, an ecosystem of scale up cyber security providers that already work in partnership is far easier and more effective to scale than starting anew.

Global providers and their related advocates are often overconfident in their beliefs that data localisation considerations are naïve, and any limitations are an unnecessary restriction to trade, with the self-interest soft strategies that seek to encourage "safe and secure data flows" to enable the adoption of cloud technologies. However until the risks associated with unfettered and unencrypted flows of support data, monitoring data and metadata are assessed and understood, until the unknowable risks relating to access to customer data and other data types by unknown overseas persons and until the emerging privacy and cyber security risks from the invasive application of AI and MI to all this Australian citizen data are fully understood and transparently addressed, we would contend that data localisation is for many data sets a critical consideration for a Government in building a sovereign cyber capability for and on behalf of its citizens.

In conjunction with the Made in Future Australia Office within Department of Finance, we recommend that the Minister's office confirm a procurement strategy for retaining, growing and enhancing the existing cyber ecosystem capability. As a minimum, this should include an immediate mandate to procure vendor resilient backups across all Government agencies and critical infrastructure providers, which would provide an immediate risk reduction for most organisation agencies and simultaneously uplift their Essential Eight Maturity posture.

Stronger Domestic Capability

Growing the domestic ecosystem feeds the soul of Australians old and young, especially the young. It attracts them to the industry, attracts them to a career and changes the profile of Australia's position in the region and globally. It also amplifies the communication of best practice to improve national resilience through their personal networks and influence on the behaviour of their family, friends and colleagues.

The problem statement for building, growing and nurturing domestic skills and experiences are well understood and the current and future skills gap regularly documented[5]. The key challenges can be summarised as:

- Building the talent pool through education at earlier stages in the curriculum and inspiring more people to consider the career opportunities of the embryonic and fast developing cyber security sector;
- Growing the inbound pipeline through re-training and/or immigration from existing experts; and,
- Nurturing and retaining the existing community through exposure to wider experiences, tools and techniques to improve their tradecraft.

The pace and growth rate for each element can be significantly enhanced not only by reducing the bias away from tertiary qualifications, STEM subjects and gender stereotypes but also by seeking talent across a more diverse (gender, ethnicity, health ability, neurodiverse) population and effective mentoring to improve retention. A non-exhaustive list of programs that have been established within the Australian provider eco-system, which focus on all these areas includes: recruitment

[5] https://cybercx.com.au/cyber-skills-report/

diversity (CYNAPSE[6]), mentoring (OKRDY[7]), inspiring talent (Cyber Taipan[8]), micro-credentials (Purple Team[9]).

The ability of all organisations to comply effectively with management and ongoing efficient maintenance of any legislative, regulatory or best practices changes merging from the updated Cyber Security Strategy will only be achieved through a combination of people, process and above all technologies. New business models will emerge that support data minimisation, enable consent management for individuals and facilitate an increasingly complex world of ADM (automated decision making) driven by API (application programming interface) centric, micro-service based applications and underpinned by inferred data. There is every reason that as a strong sovereign cyber ecosystem develops and builds capabilities to address this future, that it can become a leader in thought, technology and practice.

It is therefore imperative, that the legislation is informed by, and aligns with, related technology, relevant privacy legislation, sectoral regulation, best practice standards and individual talent aspirations. These factors will create creative challenges for those setting out on a career in cyber security and will provide a compelling range of genuine experiential opportunities to build personal capability that should facilitate enhanced retention rates as well as attracting on-going and new talent.

Accelerating Best Practice

Australia has some of the most rigorous and detailed approaches to cyber security best practices for Government data security in the world. The PSPF, HCF and CAAF frameworks, the detail of ISM controls and IRAP assessment process, combined with the simple clarity of the Essential Eight provide ample signposts for Government agencies, critical infrastructure and security conscious enterprises to establish a roadmap towards Essential Eight Maturity Level 3.

Frameworks, when combined with clear indicators from the implementation and reporting implications of SONs, should provide a strong incentive to uplift across the critical infrastructure sectors and establish best practice approaches for all sectors.   Unfortunately, few organisations currently appear to possess the necessary leadership, experience or motivation to rapidly improve

[6] New program seeks to create a more inclusive cyber workforce | Riotact (the-riotact.com)

[7] New ASD partnership to deliver Women in Security Mentoring Program - OK RDY

[8] CyberTaipan - CSIRO

[9] Purple Team Australia (cybermerc.com)

their cyber maturity, which has a direct impact on the securing of Government systems and/or systems of national significance.

Ideally, Government should stand as an exemplar of cyber security. However, according to the Commonwealth Cyber Security Posture in 2022 report[10], Government agencies have a long way to go in securing Government systems. Only 11% of entities in the Cyber Posture Report reached Overall Maturity Level 2 through the implementation of Essential Eight controls, with many yet to implement basic policies and procedures (e.g. backups). This has implications for Government in building essential trust in its role as the instigator and regulator of new SONs obligations (i.e. if Government is not yet applying its own stated best practices, when obligating a wide range of industry sectors to do so, this could create a potential barrier to widescale uptake of these best practice framework)

Beyond the localised frameworks for Government and sovereign critical infrastructure organisations, there are also well established globally recognised approaches to information security, which can provide mechanisms for organisation to improve (NIST Cybersecurity Framework) and also accredit their approaches (ISO 27001) to better cyber security practice. These are well established, understood, often mandated within a global regulatory environment and a strong indicator of good cyber security practice that are adopted by larger organisations or those providing ICT services. However, we contend that Australian and global frameworks should not be mutual exclusive for the stringent requirements of Government data sets or critical infrastructure systems of national significance. Australian frameworks (PSPF, HCF, CAAF) rightly call out the risks associated with data transit, data access and overseas legislative oversight and are better designed to reflect Australian self-determination and the risk considerations and compromise consequences of unknowable access to key Australian data sets.

An area that currently appears to lack a consistency of approach to assist cyber security uplift would be enabling the large community of small and medium sized businesses across all sectors. In this regard, we would point to the Cyber Security Essentials[11] scheme operated by the NCSC in the UK, which has been in operation since 2014 and seeks to assist organisations reduce the risk of cyber compromise. The scheme is similar in many ways to the ACSC's Small Business Cyber Security Guide[12] but provides a further step for smaller organisations to improve practice and achieve credible recognition for doing so. Several alternative sectoral approaches area also in operation within Australian (e.g. Cyber Framework for the Defence Industry (CFDI), the Australian Energy

[10] The Commonwealth Cyber Security Posture in 2022 - Report to Parliament.pdf

[11] About Cyber Essentials - NCSC.GOV.UK

[12] ACSC_Small_Business_Cyber_Security_Guide_V6.pdf

Sector Cyber Security Framework (AESCSF),the Cloud Controls Matrix (CCM)). Our recommendation would be to adapt the Cyber Essentials program or one of the other schemes and amplify uptake through promotion and awareness raising utilising existing professional networks (accountants, lawyers) or peak industry bodies (Australian Institute of Company Directors, Law Societies, Small Business Association of Australia, specialist sector associations etc.)

A key factor affecting the lack of consistency in the implementation of best practice relates to the motivation inherent within organisations to prioritise the resources and investment and bring the necessary organisational focus. There are many examples of legislative and regulatory compliance sticks. When combined with the personal or corporate self-interest of avoiding negative media headlines following a cyber incident, this should be motivation enough for organisations to accelerate cyber investment and reduce their threat vector. Conversely, there are numerous positive reasons to accelerate progress from securing competitive advantage to gain market share through to reducing the likelihood of compromise because threat actors recognise the inherent difficult of breaching your environment and move onto easier targets. And yet we still see many organisations, Government included, crowding out cyber security investment decision with other priorities.

We recommend a dual track strategy that also rewards success but progress in process not outcomes. Progress for example, against the Essential Eight Maturity framework, NIST Cybersecurity Framework, the Cyber Security Capability Model or similar maturity frameworks and ensuring that such progress is wired into Government and critical infrastructure procurement. Results for all organisations should be published and made transparent. Government must demonstrate leadership and hold itself to account in the same way. There are possible unintended consequences with transparent publication of such information but if the vision is to be achieved, transparency is the best tool in the armoury for creating longer term and sustainable change to become and maintain a world leading sovereign capability.

Acting with Pace and Adaptability

Threat actors are not waiting around for countries, organisations and/or individuals to uplift their cyber security posture and reduce the risks of data compromise. Simultaneously the context of digital dependency becomes ever more complex and technologies in emerging fields (quantum, artificial intelligence, biotechnologies, robotics, etc) bring even greater complexity to the field of cyber security professionals. Consequently, defensive responses need to address adaptability

To achieve the outlined vision, the Strategy must be adaptable to account for changes in the strategic and technological environment in the coming years. Historically, a key challenge for all organisation, especially large bureaucracies, is the ability to act quickly and adapt to changing circumstance. However, one outcome of the recent pandemic is that all organisations now have recent corporate memory in acting with pace and agility. A trait that will be a defining characteristic of world leading cyber nations in the future.

The question is how do we retain and finesse this memory muscle and avoid returning to the norm? It will certainly require a way of thinking and oversight that Governments are not renowned for; it will require adsorbing failure, avoiding blame but focusing on the learning and then adapting to avoid future failure. It will require the willingness to procure differently (but retain transparency of process as probity not the process itself), to validate return differently (pricing in the human impact of data compromise not simply the financial operational cost of the solution, service and/or technology) and to delegate authority of decision making (within an ethically validated data security framework).

We recommend that a diverse selection of representatives (Government/ enterprise/ academia, small/medium/large, urban/rural) and individuals are invited to establish an inter-disciplinary group of practitioners to assess recommendations for adapting process and the tolerance of behavioural boundaries for how Australian should address current and future risks.

RESPONSE TO SPECIFIC QUESTIONS

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

AUCloud believe Australia requires a mixed economy of global, national and local technology providers to support and protect all parts of our economy, from our international trade activities through to those activities and operations critical to Australia’s democracy, national security and indeed sovereignty.

We believe that successful achievement of the outlined vision will be underpinned through focus on five key areas to cement a strong cyber security foundation, building a resilient cyber workforce and position Australia as a global leader in security:

6. **The importance of ‘Defining Data’** - in terms of both security and privacy, there is a fundamental requirement for one common and meaningful definition across both public and private sectors, which aligns cyber security, privacy and procurement’s contractual considerations.
7. **Sovereign Resilience** - increased focus on true sovereign resilience, control and governance to protect Australian interests and critical infrastructure, to foster a vibrant domestic ecosystem and in turn to drive Australian intellectual property (IP) and reputation across the global cyber security industry.
8. **Stronger Domestic Capability –** mechanisms and policies to help stimulate, foster and grow a critical workforce for the industry, supporting the domestic economy, security and international partnerships.
9. **Accelerating Best Practice behaviours –** better promotion and enhanced adoption of existing security, assurance and privacy frameworks and behaviours can not only help uplift the cyber capability of Government, critical infrastructure and large enterprises but also secure data and increase resilience of SMEs and individual citizens.
10. **Acting with Pace and Adaptability –** whether in the context of more invasive, broad based, cyber compromise or the adaptation of new technologies, threat actors and the world are not waiting for anyone to catch up or develop policy, therefore a change of pace for hastened improvement and openness to adaption will be essential to success.

In recent times the ACSC has often referenced a ‘whole of economy’ approach to achieving cyber security goals. It is increasingly important that the Government and their delivery agencies deliver upon domestic capabilities for Australian businesses at all levels. An important factor in the success or otherwise of any new strategy will be Government's ability to recognise themselves, and act like, a service provider to Australia, and not just an information provider.

2. What legislative or regulatory reforms should the Government pursue to enhance cyber resilience across the digital economy?

We believe there are already sufficient legislative and regulatory controls in place to enhance cyber resilience. However, we contend that a key issue for achieving the desired vision is more about meaningful oversight in the implementation of existing frameworks combined with effective application of the related sanctions. There are two areas that we could call out that are partly legislative and partly operational implementation:

- Firstly, Government must ensure alignment with the impending update to Privacy legislation, which is essentially the 'Confidentiality' pillar of information assurance, in particular, definitions relating to 'Data' (in all its forms) and 'Personal Information'.
- Secondly, Government must show leadership by accepting and undertaking similar cyber security obligation on itself, that it is demanding of others through SOCI and other legislative levers.

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)?

Legislation can be and is effective in improving mandatory standards across the economy. However, Government will continue to require ongoing consultation and engagement with industry across a wide variety of sectors to achieve the desired outcomes. With different sectors at varying levels of cyber maturity, standards will rarely be a one size fits all so Government will need to remain flexible and maintain firm interest in the development and maturity of different industry sectors.

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?

Yes. We believe that the ultimate unit of protection is the IP packet and the data contained therein and therefore the underlying data should be defined in detail and included within the definition of 'critical assets". This would not only be the physical customer data but also the account data, the metadata and the support and administrative data since all these inherent data types provide vectors of compromise of the confidentiality, availability and integrity of both the data and overall system.

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

Directorial fiduciary obligations already implicitly address cyber security risks and consequences as they do with each and every other business risk. The unique challenge with cyber security is that it is potentially an existential force majeure event, albeit one that can be mitigated by best practices. Our contention is that corporate reporting of actions to mitigate cyber security risk should be mandated to be communicated as frequently and as effectively as financial reporting. This would establish greater transparency for investors, customer, suppliers and other stakeholders to determine that company directors are seen to be understanding, addressing and mitigating the potential cyber security risks.

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

A Cyber Security Act could be considered necessary based upon the frequency, consequence and impact of cyber-attacks. However, without having any understanding of the proposed intent or context beyond existing legislation it makes it difficult to provide a meaningful contribution.

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

The regulatory regime around cyber security is undoubtedly becoming more burdensome across the whole economy not only in the quantity of reporting obligations but in the complexity and inter-relatedness. Certain obligations are input based (IRAP for Government, HIPAA for healthcare, PCI DSS for credit card transactions, etc) and are mandated as proxies for best practice to achieve outcome obligations (breach notification for SONs, impending breach notification for Privacy, ASX/ASIC reporting, change notifications within Hosting Certification Framework, etc). However, in addition to specific cyber security related requirements, there are numerous regulators who require the same information in a slightly different form, within a slightly different timescale, which all add to the regulatory burden for businesses. It would be of great assistance and likely improve effectiveness if information reporting requirements were better aligned

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?

(i) What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

Arguably it is already illegal in Australian to make payments to a criminal organisation, albeit mitigated, for example, by threat to life and/or duress. It becomes an interesting point of contention as to whether the cyber-criminal, the victim or your insurer is the source of duress. The principle of such legislation would be that if payments are criminalised for any reason then this would make Australia a less attractive market for criminal concerns as it would reduce their return on investment. The moral argument would be that this would push the activities into near digital neighbours equivalent to a burglar alarm in a street pushing crime to those without obvious alarms. Furthermore, in some circumstances, there would almost certainly be unintended consequences from the duress that this could place people in, especially in a life-threatening situation.

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?

Notwithstanding the response to the above question (f), it would be beneficial for Government to clarify under existing legislation, the considerations for individuals or company directors relating to ransom payments to limit the areas of uncertainty.

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

Australia adopting a leading position within the region to reduce risk and the attack surface of our neighbours would be a worthwhile ambition. Resilience within the broader region will provide confidence and opportunity for the Australian technology industry to grow. Depending on the nature of the relationship that parties are mutually seeking and their respective level of cyber maturity, there are different activities that can be undertaken to work with neighbours, from mutual threat intelligence sharing, delivery or participation in educational/training programs or more active uplift support through service delivery or secondments.

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

No comment to make.

5. 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?

For the most part Australia is already considered forward thinking regarding our approach to cyber security. Where we have lacked is the implementation of such standards, especially across sectors such as Government and Defence who for many years have failed to implement the cyber security basics that they themselves created. For Australia to effectively contribute to these conversations, it is imperative that the Government leads by example.

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

The SOCI legislation and associated SONs regulations creates some significant obligations for affected organisations to which Government rightly expects to hold them to account. It would be a material signal of commitment and leadership, were Commonwealth Government to hold itself to the same level of compliance and disclosure and apply the obligations to Commonwealth Government and related entities.

One simple example of intent to deliver on the Essential Eight maturity framework, would be for every Government entity to commit to securing vendor resilient backups and recovery capability for its core data.

7. What can Government do to improve information sharing with industry on cyber threats?

Improve the effectiveness of the cyber threat intelligence sharing program, which has been built a considerable expense. The program will require expansion (ideally on sovereign infrastructure given the national sensitivity and importance of the data) and considerable trust building to ensure wide-spread mutual participation.

8. 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?

This question raises far greater issues and consideration about behaviours that occur during incidents across multiple parties. These actions are likely driven by different legal, regulatory and national leadership obligations but often do little to contribute to the resolution of an incident. This could be especially challenging as investigations unfold and information asymmetries between parties emerge.

9. 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?

Potentially but it would certainly require a considered and timely public information and education program to provide greater contextual information to ensure that neither scaremongering nor indifference were the result.

10. What best practice models are available for automated threat-blocking at scale?

National scale IWF blocking through to PDNS services or commercial services (Cisco Umbrella) are all effective technical solutions for blocking internet traffic and related threats. However, the philosophical and moral challenge for an open democracy is by whom (organisation or individual) and on what basis the decision is made as what URLs, traffic or perceived threats are automatically blocked.

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

The problem statement for building, growing and nurturing domestic skills and experiences are well understood and the current and future skills gap regularly documented. The key challenges can be summarised as:

- Building the talent pool through education at earlier stages in the curriculum and inspiring more people to consider the career opportunities of the embryonic and fast developing cyber security sector;

- Growing the inbound pipeline through re-training and/or immigration from existing experts; and,
- Nurturing and retaining the existing community through exposure to wider experiences, tools and techniques to improve their tradecraft.

The pace and growth rate for each element can be significantly enhanced not only by reducing the bias away from tertiary qualifications, STEM subjects and gender stereotypes but also by seeking talent across a more diverse (gender, ethnicity, health ability, neurodiverse) population and effective mentoring to improve retention. A non-exhaustive list of programs that have been established within the Australian provider eco-system, which focus on all these areas includes:

- Recruitment diversity (CYNAPSE)
- Mentoring (OKRDY)
- Inspiring talent (Cyber Taipan)
- Micro-credentials (Purple Team)

12. What more can the Australian Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

See response to Question 11.

13. How should the Government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

a. Should Government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

Putting aside the nuance of how to determine what factors escalate an incident into a major cyber incident, Government has several tools and capabilities available to it that no commercial organisation can replicate. Most of these capabilities fall into law enforcement or operational considerations. Additional activities would relate to:

- Facilitating reporting of incident to improve efficiency for organisations to discharge their multiple legal and regulatory obligations.
- Capturing information on incidents, including near miss major incidents, to provide, for example, longitudinal data trends on scale, rate and nature of events and their causes.

- Undertaking analysis on behalf of sectoral and the whole community and hosting events to support knowledge sharing and wider capability uplift

14. What would an effective post-incident review and consequence management model with industry involve?

One of the most effective, well understood and consistently applied incident learning models, free from political or other influence, is that operated across the international airline industry. This seeks to identify root cause of incidents, including near misses, and apply the learnings to mitigate risk and avoid such incidents reoccurring. It is not a complete match for addressing cyber security as the scale, speed and relentless nature of the cyber security attacks are very different from the root cause errors that typically trigger incidents within the airline industry.

15. How can Government and industry work to improve cyber security best practice knowledge and behaviours and support victims of cybercrime?

a. What assistance do small businesses need from Government to manage their cyber security risks to keep their data and their customers' data safe?

As an immediate action, Government could mandate the requirement to ensure data backups for all key organisational systems. It is a basic activity that far too many organisations choose to ignore.

Several years ago, the UK Government introduced the Cyber Essentials scheme to guard against the most common cyber threats and demonstrate an organisations commitment to cyber security. A similar scheme in Australia, at a non-restrictive price point, would allow a large variety of organisations to not only uplift their cyber security knowledge but also promote their commitment to cyber security principles.

The scheme is similar in many ways to the ACSC's Small Business Cyber Security Guide but provides a further step for smaller organisations to improve practice and achieve credible recognition for doing so. Our recommendation would be to adapt the Cyber Essentials program or one of the other schemes and amplify uptake through promotion and awareness utilising existing professional networks (accountants, lawyers) or industry bodies (Australian Institute of Company Directors, Small Business Association of Australia, specialist sector associations etc)

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

As the single largest potential and most credible customer in the eyes of the external investment community, Government has a pivotal role to play to enhance Australia’s domestic cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia. It is one of the single largest and most credible customers when it comes to data and security in the country, and its influence on encouraging external investment cannot be overstated. Government procuring services from Australian owned companies begets external market investment, which begets a growing and virtuous ecosystem of cyber security capability. Procuring not for any feel-good patriotic duty, but because existing going-concern Australian companies across the cyber security ecosystem are more than capable of delivering and supporting national scale, high-risk, high-profile services for Government and critical infrastructure in-country, without cause or need for overseas personnel accessing Australian systems. Furthermore, an ecosystem of scale up cyber security providers that already work in partnership is far easier and more effective to scale than starting anew.

In summary, ignore the temptation to commission another review, ignore the advisors whispering that this creates a procurement risk and if for no other reason than the national security consideration that you don’t want your data transmitted offshore for unknown people to access, then spend more money and buy more services from the existing going-concern companies that already deliver high profile, cyber secure services to Australian organisations.

17. How should we approach cyber security technologies future-proofing out to 2030?

Threat actors are not waiting around for countries, organisations and/or individuals to uplift their cyber security posture and reduce the risks of data compromise. Simultaneously the context of digital dependency becomes ever more complex and technologies in emerging fields (quantum, artificial intelligence, biotechnologies, robotics, etc) bring even greater complexity to the field of cyber security professionals. Consequently, defensive responses need to address adaptability.

To achieve the outlined vision, the strategy must be adaptable to account for changes in the strategic and technological environment in the coming years. This requires the willingness to procure differently whilst retaining transparency and rigor of process for probity, to validate return on investment differently (pricing in the human impact of data compromise not simply the financial operational cost of the solution, service and/or technology) and to delegate authority of decision making (within an ethically validated data security framework).

We recommend the appointment of a diverse selection of representatives (Government/enterprise/academia, small/medium/large, urban/rural) and individuals are invited to establish an inter-disciplinary group of practitioners to assess recommendations for adapting process and the tolerance of behavioural boundaries for how Australian should address current and future risks. The group should be a permanent activity, but the participants should hold 2-3 year terms and the individuals should be Ministerial appointments not defined by their existing roles.

18. Are there opportunities for Government to better use procurement as a lever to support the Australian cyber security technologies ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

See response to Question 16. The simple answer is Yes. We welcome the opportunity to discuss several ideas about how this can be achieved even within the perceived self-imposed constraints of Government procurement rules.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security-by-design in new technologies?

See response to Question 17.

20. How should Government measure its impact in uplifting national cyber resilience?

The key measures should be focused on progress in process and not the number or scale of events within a given period. Resilience is a societal change activity and will become even more challenging with the emergence of AI/ML, quantum technologies and broader societal dependence on a greater scale or even more invasive technologies. In summary our dependency on data will grow and cyber security is all about how we protect the confidentiality, availability and integrity of that data.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

Regular and consistent reporting of chosen KPI metrics that are not changed when they become politically unpalatable, with explanations of the good and bad.