15th April 2023

The Hon Clare O'Neil MP
Minister for Home Affairs
Minister for Cyber Security
Australian Department of Home Affairs

Subject: Priorities for the 2023-2030 Australian Cyber Security Strategy

Dear Dear Minister O'Neil,

We are writing in response to the discussion paper published by the Expert Advisory Board on 27 February 2023 regarding the Priorities for the 2023-2030 Australian Cyber Security Strategy to provide industry views on how the technology sector can work together in making Australia a world-leader in cyber security by 2030. Vault has vast amounts of experience dealing with the issues raised in the Discussion Paper and providing responses based on the available information. Therefore, we are pleased to share our expertise on this discussion with the Home Affairs' Cyber Security Strategy Expert Advisory Board.

We understand that one of the primary roles of the Home Affairs is to ensure the safety and security of Australia and its citizens, including counterterrorism, intelligence, and cyber security operations. To make Australia a world-leader in cyber security by 2030, regulatory oversight, controls and rules must be dramatically strengthened. These reinforcement efforts must focus on: enhancing the economy and the cyber ecosystem; ensuring resilient and secure critical infrastructure and government systems; increasing our sovereign and reliable capacity to counter cyber threats; and establishing ourselves as a trusted and influential global leader in fostering a cyber resilient region.

Secure Economy and Thriving Cyber Ecosystem

The Financial Services Sector is well established, regulated and some assets are deemed Critical Infrastructure. Most consumers would agree that a trusted, predictable and regulated Financial Services sector is preferable to an unregulated wild west. Both Financial Services and the Data Storage and Processing Sector (Data Sector) often lobby for deregulation, however under the previous government, unfortunately, we saw the deregulation efforts succeed. The ASD was Australian de facto Data Sector regulator until their withdrawal in July of 2020.

In March 2020 Vault Cloud, on the public record, in the media and in direct representations to the previous Government, warned of the catastrophic consequences of ASD's exit as a regulator from the Data Sector without a new regulator. Unfortunately, we have all lived through recent events and felt the consequences.

We welcome the new Government's approach, both in the appointment of a member of Cabinet with accountability for Cyber Security and the Department of Home Affairs making inroads on regulating the Data Sector. However additional action is required. To highlight the gaps, we have outlined some comparisons to other sectors.

Sector	Finance	Aviation	Data
Australian Sector Formation	1817	1910	1987
Australian Regulator Formation	1959 and earlier	1998	2015-2020 2022-current
Current Regulator	Australian Prudential Regulation Authority	Civil Aviation Safety Authority	A small section of The Department of Home Affairs
Dedicated Sector Regulator	Yes	Yes	No
Number of personnel employed by the regulator	>600	>800	<25 FTE estimated - No published data
Significant Sector Risks	Economic damage	Mass loss of life	Mass loss of life, economic damage, National Security, sovereignty
Sector Risk Performance	Strong	Strong	Weak
Sector Domestic Standards	Strong	Strong	Strong

We believe that, like other sectors, a well regulated Data Sector is essential to a secure economy and a thriving cyber ecosystem. We submit that the Data Sector is gravely underregulated.

Recommendation:

1) Establish an independent Data Sector Regulator that is comparably empowered and funded to other regulators such as APRA and CASA.

The National Reconstruction Fund (NRF) represents a substantial amount of capital that has the potential to greatly enhance Australia's Cyber Security Capability. By allocating funds to develop and support cutting-edge cyber security technologies, infrastructure, and training programs, the NRF can play a crucial role in strengthening the nation's defence against cyber threats.

Investing in this area not only ensures the protection of critical infrastructure and government systems but also promotes the growth of a thriving cyber ecosystem. Furthermore, by fostering innovation and encouraging collaboration between the government, academia, and the private sector, the NRF can help Australia become a global leader in cyber security, attracting top talent and promoting a resilient digital environment for businesses and citizens alike.

Recommendation:

2) Prioritise NRF funding towards Cyber Security investments

The Buy Australia Plan and the Future Made in Australia Office (FMiAO) are strategically positioned to enhance Australia's Cyber Security Capability. By prioritising the procurement of locally developed and manufactured Cyber Security products and services, these initiatives can stimulate the growth of the domestic Cyber Security industry, fostering innovation and competitiveness. This, in turn, can lead to the creation of more high-quality jobs and opportunities for skilled Australian cyber security professionals, ultimately reducing the risk of brain drain to multinational corporations.

The Buy Australia Plan and FMiAO can facilitate the transfer of cutting-edge knowledge and technologies, ensuring that Australia remains at the forefront of global cyber security advancements. These initiatives, when combined, have the potential to make a significant impact on Australia's ability to protect its digital infrastructure, defend against cyber threats, and establish the nation as a trusted leader in the global cyber security landscape.

The National Data Security Action Plan (NDSAP), as a driver of digital security and part of the Digital Economy Strategy, is a critical trust and protection measure in the Australian Data Strategy. To have a clear guidance on data sovereignty requirements to increase reliable investments from both global and domestic providers, it needs a unifying role with the current Government Buy Australian Plan and the NSW Government Sovereign Procurement concept of retained economic benefit and value for money.

Recommendations:

3) Align the 2023-2030 Australian Cyber Security Strategy with the Buy Australia Plan and FMiAO.
4) Set a target that 80% of Government spend in the Data Sector should be made in Australia

REDSPICE is the most significant single investment in the Australian Signals Directorate's 75 years. $10B is a sufficient amount of funding to transform Australia's Sovereign Cyber SecurIty capability if used correctly. We are concerned that, to date, all of the funding has been used to hire capability within ASD, resulting in a brain drain from Australia's Cyber Security workforce. If REDSPICE were to purchase Australian Sovereign Cyber Security capability, it would have the dual benefit of supporting the objectives of the program and growing Australian Sovereign Cyber Security capability.

Recommendation:
5) Refocus REDSPICE spending away from direct headcount and towards Australian Sovereign Cyber Security capability

SOCI Act Reforms and Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 put additional cyber security obligations, funding and structural changes on critical infrastructure assets. The Government should use the forthcoming reform of the SOCI Act as an opportunity for a more proactively approach towards operators of System of National Significance (SONS), critical infrastructure providers and Government agencies.

Recommendation:
6) Publish a list of trusted sovereign providers to key stakeholders including SONS (In relation to recommendation 10)

During World War II, car manufacturers Ford and Volkswagen were repurposed to support the Allied and Axis powers. Cyber is the fifth domain of warfare and Sovereign Cyber capabilities are also often "Dual Use", generating economic benefit in peace time and providing National Security in war time. Free trade agreements acknowledge the importance of national security and permit prioritised procurement to address these concerns.

Recommendation:
7) Update the definition of Value for Money in the Commonwealth Procurement Rules to include Retained National and Economic Benefit

Vault Cloud supports the AIIA's Domestic Capability Framework Policy in full[1].

Recommendation:
8) Implement the AIIA's Domestic Capability Framework Policy in full

To give Australian citizens and businesses the confidence to fully engage in the growing digital economy, Australia should be seen domestically and internationally as a nation with mature cyber security against other countries and there is a pronounced open and engaged approach from the Government to drive regulatory reforms and uplifts through critical infrastructure.

[1] https://aiia.com.au/wp-content/uploads/2021/06/AIIA-DC-Framework-Policy-2021-1.pdf

Secure and Resilient Critical Infrastructure and Government Systems

Vault Cloud is in many ways the brainchild of ASD and Defence. We have experienced first hand how a regulator with high standards is able to drive an organisation to Cyber Security excellence. ASD and Defence further improved Vault's capabilities not just through regulation but also as a supportive collaborator and as subject matter experts.

Vault has implemented many standards including:

- Top 4
- Essential 8
- Information Security Manual (ISM)
- Protective Security Policy Framework (PSPF)
- Defence Security Principles Framework (DSPF)
- Several ISO standards
- Several NIST standards

When we look back with the benefit of hindsight, it is clear that the Australian standards provided Vault with the vast majority of Cyber Security protection and the international, US and UK standards were of marginal efficacy. As far as we are aware there has never been a Cyber Secuirty incident involving a system that was 100% compliant to the ISM. There have been many thousands of incidents involving systems that are certified to foreign and international standards.

To realise our goal of becoming the world's most cyber-secure nation by 2030, it is crucial that Australia assumes a leadership position, rather than a subordinate one.

Recommendation:

9) Continue investing in: Top 4, Essential 8, Information Security Manual (ISM), Protective Security Policy Framework (PSPF) and the Defence Security Principles Framework (DSPF) to keep Australia as a world leader

Sovereign and Assured Capability to Counter Cyber Threats:

If a lesser known Cyber Security brand has a major breach, it is likely to be terminal for the organisation. If a major brand like IBM has a breach, it is unlikely to be terminal. Yet if a lesser known brand claims that a product is secure it will be met with scepticism where a Brand like IBM can go unquestioned. The over 200,000 records in the Common Vulnerabilities and Exposures (CVE) database provide an overwhelming proof that this common human behaviour is not evidence based.

In other words, Australian brands need a trusted way to demonstrate their security credentials to allow them to compete with global brands.

Recommendations:

10) Fund a Government program to transparently assess, assure and certify Australian Cyber Security products compliance against Australian standards
11) Mandate the National Anti-Corruption Commission (NACC) to have a role maintaining the integrity in certification activities

Data sovereignty refers to the concept that data is subject to the laws and governance of the country in which the data originated.

In order of importance, the main sub constructs of data sovereignty are:

- Legal - the data is subject solely to the laws of the country of data origin. Generally, this means that the custodian must be owned and operated within the country.
- Operational - data, metadata, monitoring and remote access are managed solely within the country of the data's origin.
- Physical - the data at rest and in transit remains within the originating country.

We support the need for an explicit approach to data localisation and sovereignty.

When in-country data is stored on services, which are subject to foreign laws, an organisation retains substantial legal obligations concerning that data's protection. However, the information may no longer be under their control and could be impacted by the laws and actions of a foreign country. This includes the future (as yet unwritten) laws of a foreign country. While the privacy laws of foreign countries may align to Australia's today, there is no certainty that they will do so in the future. At present, some countries have sectoral coverage, while others have omnibus law, with at least one national data protection law in addition to sectoral regulations. In Europe, under GDPR a citizen must be informed if their data is subject of foreign law and have the right to opt-out of non-sovereign services.

Sovereignty is a growing consideration in many countries. Canada, USA, UK, Germany, China and many other countries have strong sovereignty requirements and capabilities.
Interestingly in the United States, home to many public cloud services, the US Government does not allow the use of public clouds for sensitive data. Instead they elect to use special sovereign variants known as "Government Cloud", "Community Cloud", "Sovereign Cloud" or "Secure Cloud".

In the first draft of the Digital Transformation Office's (DTA) Hosting Certification Framework (HCF) there was a status called "Sovereign Certified". This status was subsequently removed.

We believe that buyers should be able to understand if a product or service is sovereign.

Recommendations:

12) Update the DTA HCF to include a Sovereign Certified status
13) Refer the removal of the Sovereign Certified status to the National Anti-Corruption Commission (NACC) and the AFP to investigate foreign interference

The Australian Government has legislated that Qantas, an airline and Telstra, a telecommunication provider must remain sovereign. Yet, no equivalent legislation exists in the Data Sector.

Foreign special interest groups would argue that Sovereignty of the Data sector would increase rent seeking and does not improve National Security. Yet the ACCC has an ongoing investigation into activities that would be described as rent seeking from "Big Tech". The recent withdrawal of Microsoft from the classified part of the Data Sector and the decision from IBM to close its Melbourne Data Sector region very much show that decision can be made offshore without consultation that directly impacts Australia's Cyber Security capability.

Further, there is an aggregation risk posed by the Data Sector. If Qantas and Virgin both use the same provider from the Data Sector, and that provider is subject to an adverse decision made outside of the jurisdiction of Australia, it is conceivable that the majority of Australia's aviation capability will be inoperable for an extended period.

Clearly the amount of sovereignty required from the Data Sector for a classified military system and a social media platform like TicToc are not the same. Vault is very supportive of foreign investment in the Data Sector and clear guidance would provide the Data Sector certainty for both domestic and foreign investment.

Recommendation:

14) The Government should provide clear guidance on Sovereignty requirements for consumers of the Data Sector

Australia as a Trusted and influential Global Cyber Leader

Many of Australia's neighbours have a distrust of both American and Chinese Cyber Secuirty products and services. However both the US & China subsidise their companies and directly assist those companies to penetrate our regional neighbours markets.

Our experience is that Australia's neighbours would prefer to buy Australian Cyber Security products and services, including Vault Cloud, over other jurisdictions. We see two prerequisite for success:

- The Australian Government needs to buy Australian products to show that they are credible, and
- The Australian Government needs to directly stand behind Australian companies in discussions with regional neighbours

A growing number of Australian companies have developed beyond the start-up phase to become internationally competitive while supporting economic growth and jobs at home like well-known companies such as Atlassian and Afterpay and emerging firms such as Willow, Culture Amp and AgriDigital. To lift up the capability of Australia, we need leadership, capital, tax reform, legislative changes, policy making, and the proactive use of government buying power.

It is our view that if the Government does not take intervening action, other countries will successfully and irreparably displace Australian technology out of our region neighbours.

Recommendation:

15) Once Australian Cyber Security Capabilities are credible, the Government should directly assist Australian companies to negotiate with regional neighbours

AUKUS, the trilateral security partnership between Australia, the United Kingdom, and the United States, presents both opportunities and challenges for Australian Cyber Security. On one hand, the partnership offers Australia access to advanced cyber security technologies, intelligence sharing, and cooperation with two of the world's most technologically advanced nations. This collaboration can help strengthen Australia's cyber defences and facilitate the development of new capabilities to counter emerging cyber threats. Furthermore, working closely with the UK and the US can provide opportunities for Australian companies and professionals to participate in joint projects, enhance their skills, and expand their global networks.

On the other hand, the AUKUS partnership may pose certain risks to Australian Cyber Security. The balance of trade within the agreement thus far appears to have been more favourable to the UK and the US than to Australia. This imbalance could lead to increased reliance on foreign technologies and services, potentially undermining the growth and competitiveness of Australia's domestic cyber security industry.

In order to fully capitalise on the benefits of the AUKUS partnership while mitigating its potential risks, Australia must carefully navigate its involvement, ensuring that the interests of its cyber security sector are adequately protected and promoted. This could involve advocating for more balanced trade

arrangements, supporting local businesses in accessing international markets, and investing in the development and retention of Australian cyber security talent.

Recommendation:

16) The Government should ensure that Australia exports at least as much Cyber Security capability to the US and UK as it imports

Summary

Ensuring a secure economy and thriving cyber ecosystem is of paramount importance for Australia's national security and prosperity. By implementing the recommendations provided, the Australian Government can take crucial steps to strengthen its Cyber Security capabilities, bolster domestic industry, and protect against potential threats. By focusing on developing a well-regulated Data Sector, prioritising investments in Cyber Security through the NRF, aligning national strategies with the Buy Australia Plan and FMiAO, and fostering domestic talent and innovation, Australia can become a global leader in Cyber Security.

Additionally, addressing the challenges and opportunities presented by AUKUS and the evolving cyber landscape will be essential for maintaining Australia's position as a trusted and influential global cyber leader. The government must strike a balance between international collaboration and fostering domestic capability, ensuring that Australia's Cyber Security capabilities are not undermined by external factors. By acting decisively and strategically, Australia can achieve its vision of becoming the world's most cyber-secure nation by 2030, creating a safe and resilient digital environment for generations to come.

We look forward to participating in the execution of the 2023-2030 Australian Cyber Security Strategy.

Sincerely,

Rupert Taylor-Price
CEO