VeroGuard
Systems

13 April 2023

<u>Submission to the 2023-2030 Australian Cyber Security Strategy Discussion Paper</u>

VeroGuard Systems welcomes the opportunity to provide its submission to the 2023-2030 Australian Cyber Security Strategy Discussion Paper.

The paper will be a critical milestone in helping achieve the Australian Government's vision to become the most cyber secure nation in the world by 2030.

As an all-Australian company focussed for the past two decades on creating sovereign solutions to one of today's biggest global problems – cybercrime – we're pleased to offer our observations for consideration by the Advisory Board and other relevant parties.

We welcome any questions or queries on this submission and thank the Department of Home Affairs for this opportunity to contribute to the Discussion Paper.

[redacted]

H. Daniel Elbaum
Chairman and Co-CEO
VeroGuard Systems Pty Ltd

About VeroGuard Systems
With over 100 years of combined experience in the fields of network security and digital commerce, VeroGuard Systems is headquartered in Melbourne, Victoria and has a manufacturing plant in the Edinburgh defence precinct in Adelaide, South Australia.
The VeroGuard platform was initially developed and patented by H. Daniel Elbaum in 2003. Almost two decades on, the platform has successfully brought interbank and defence-grade certified security protocols to open internet networks – a global first.
The platform creates an ultra-secure ecosystem of trusted members for ID authentication, sharing, transacting, storing, communicating and using data. As a result, any unauthorised access to cyber systems and data (by either humans and machines) is prevented.

VeroGuard Systems Pty Ltd
ABN 25 617 573 001

[redacted]
Web: www.veroguard.com.au/

1. A National (and International) Problem

The Australian Cyber Security Centre's (ACSC) 2021-22 Threat Report states that one cybercrime incident is reported on average every seven minutes (or more than 76,000 cybercrime threats to Australian organisations that fiscal year). The problem is clear, present and costly.

While the Medibank and Optus breaches received the highest public profiles, other attacks occurred in 2022 at companies and departments including (but not limited to) Woolworths, NDIS, the AFP, The Smith Family and Telstra. So far in 2023, other notable breaches have occurred at Latitude Group and Crown Resorts.

With not all cybercrime reported, it's likely that what we have witnessed to date is the tip of the iceberg. Australia is part of a major international problem.

2. The Need for a National Approach

VeroGuard supports the objective to co-ordinate and support a national approach to tackling cybercrime in Australia.

From a public sector perspective, such an approach would be advisable across Federal, State and Local jurisdictions. Measures to protect the private sector (large, medium and small Australian business) and Australian consumers should be as cohesive as possible.

A consistent national approach will provide Australia with a secure economy and thriving cyber ecosystem. It should be underpinned by a commitment to protect and prevent, rather than the current reactive strategy of detect and remediate.

3. Sovereignty Should be Mandatory

Over the past few years it has become clear that Australia's cyber security future must have sovereignty capability.

Deputy Prime Minister and Minister for Defence Richard Marles' statement to the House about sovereignty on Feb 9, 2023, underlined the mission of safety, security and sovereignty:

"The first responsibility of government is to provide for the safety and security of its people… But at the heart of this compact is sovereignty – The capacity of a people, through their government, to determine their own circumstances and to act of their own accord, free from any coercive influence...
Expanding cyber and grey zone activities are blurring the line between peace and conflict."

The cyber theft of ASIO's building plans in 2013 and the more recent security risks to Government buildings and assets posed by Chinese-manufactured CCTV cameras (March 2023), reinforce the view that end-to-end home-grown approaches (including solutions) must be prioritised, if not made mandatory.

Estonia, with a population of less than 2 million people, shows how a focus on sovereign cyber security capability can deliver significant economic, security and social benefits.

4. Working in Partnership with Industry and the Community

It's crucial that separate tiers of Government not attempt to solve this issue alone.

For Australia to become a trusted and influential global cyber leader, working in partnership with local industry and strategic partners is not only sensible, but could uncover a burgeoning new economic and employment driver.

Minister for Home Affairs and Cyber Security Clare O'Neil 27 February 2023 highlighted the principles of partnership:

"As a nation, we cannot sleepwalk into our cyber future. I want Australia to be the world's most cyber secure country by 2030. I believe that is possible, but it will take a concerted effort from industry and Government alike.
"Industry needs to put cyber security at the heart of its business decisions and practices, and Government needs to walk the talk and work with industry as genuine partners to build a nationally consistent approach."

Further, Expert Lead on the Minister's Expert Advisory Board, Mel Hupfeld, said:

"Cyber resilience requires a coordinated approach by governments, individuals, and businesses of all sizes.
"When looking to 2030, Australia must consider our sovereign capabilities in cyber security and how these can be leveraged to ensure the safety and security of our citizens."

As Australia continues its journey to a more cyber secure future, local business and industry must help by innovating and delivering workable solutions. This will help assure Governments that home-grown capability and well-informed communities can effectively partner them to boost security and the broader economy as a whole.

VeroGuard believes Australia can become the world's leading cyber security location, partnering neighbouring countries and those further abroad to deliver a more globally cyber secure world.

Building a world-class local cyber security workforce, Australia would become a global net exporter of leading-edge cyber-security technologies and solutions.

While the narrative from Government on cybersecurity and manufacturing sovereignty is encouraging, we believe immediate action is required on key cybersecurity initiatives if Australia is to demonstrate cyber security best practice by 2030. The World Economic Forum future series stated in 2020 that:

"Unless action is taken now, by 2025 next generation technology, on which the world will increasingly rely, has the potential to overwhelm the defences of the global security community."

One initiative that VeroGuard supports is the establishment of **Public Private Partnerships** as a Commonwealth policy direction to help drive the development of Australian designed and made solutions deployed as sustainable, affordable and at scale.

5. Securing Access to Government Systems with Defence-Grade Hardware Protection

With Commonwealth, State and Local Governments housing some of Australia's most sensitive data, they will continue to be a major target of global cybercrime and espionage. In 2022, Australia's public sector accounted for almost 20 per cent of the nation's total data breaches.

From a Commonwealth Government perspective, just 11 per cent of entities in the Cyber Posture Report reached Overall Maturity Level 2 through the implementation of Essential Eight controls. The majority of those entities are yet to implement basic policies and procedures.

Cisco's 2023 Cybersecurity Resilience Index shows 'identity management' is the number one risk for cyber-attacks. A 2023 study by research firm Vanson Bourne also found that 69 per cent of organisations in Australia had ransomware start with phishing designed to steal credentials.

For Commonwealth Government Departments and agencies to better demonstrate and deliver cyber security best-practice and serve as a model for other entities, VeroGuard recommends that all digital identities and access be secured by defence-level certified protection, particularly when using open networks.

This would deliver clear, immediate security and economic benefits with proven ID protection that to this day has only been available on closed networks for high security environments such as inter-bank transfers and military defence systems - which have never been breached.

Hardware over Software and High-Level Certification

With software defence against cybercrime increasingly failing, Hardware Security Modules (HSMs) are now superior forms of defence.

Microsoft Research published a report this year that states how cybercrime is now 'industrialised'. Multi factor phishing kits are widely available and used, making amateur criminals sophisticated and software based authentication, including multi factors, of little or no use. Quantum computing is expected to compound this problem for software-only solutions.

Systems on closed networks that have relied on certified HSM to HSM security (as mentioned above) have still never been breached, so adapting that approach to open online Government networks would deliver significant security improvement and consequent economic benefits.

As this solution exists now, and can be implemented now, it's time to deploy this defence industry-grade solution to protect against the primary driver of cybercrime, rather than wait for marginal improvements in attempting to detect criminals. A strategy to 'protect and prevent' will always outperform that of 'detect and remediate'.

High-level certification of access solutions must be prioritised for Government and critical industries. This includes:

- **Common Criteria Certification** – Solutions that are certified for use in secure environments operated by Government and Defence across the 31 member countries - a market of over 100 million users.

- **FIDO2 Authentication**. The FIDO Alliance was created with the intent of moving the world beyond passwords, away from software tokens and passwords, towards hardware-based devices that operate out-of-band from the operating system. The FIDO2 alliance includes Microsoft, AWS, Google, IBM, Apple and Facebook as members. FIDO Authentication enables the replacement of password-only logins with secure and fast login experiences across all websites and apps.

- **PCI PTS 5.1.** The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

In addition to the above certifications, VeroGuard's VeroCard also received EMV® Level 1 certification for contactless payment system hardware on March 24, 2023, and expects Level 2 and Level 3 certification by June/July this year.

We believe the right mix of hardware and security certifications can secure Government systems like never before - unlocking significant economic opportunity and major investment in critical Commonwealth delivery areas including education, health and infrastructure.

6. Regulatory/Legislative Reforms & Conclusion

Consideration should also be given to a new Commonwealth Cyber Security Act, one which would (among other things):

a. Drive improved community awareness of how to best protect their cyber assets;
b. Ensure public and private sector holders of sensitive data have clear and consistent guidelines to honour their cyber security requirements;
c. Provide stronger governance of Australia's cyber security risks;
d. Introduce Public Private Partnership opportunities to create a viable path to market for Australian cyber security firms; and
e. Ensure sovereignty of solutions and solution affordability for large, medium and small businesses and consumers alike.

VeroGuard
Systems

VeroGuard believes Australia’s cyber security is fundamental to a strong country and safer communities.

We know the problems are vast and growing, but we’re also confident of Australia’s desire and capability to work together to find solutions which can achieve the Australian Government’s vision to become the most cyber secure nation in the world by 2030.

We thank the Department of Home Affairs again for the chance to provide this submission to the 2023-2030 Australian Cyber Security Strategy Discussion Paper.