VeroGuard Systems

25 August 2021

Department of Home Affairs

Dear Sir/Madam

Response to Strengthening Australia's Cyber Security Regulations and Incentives consultation paper

We welcome the opportunity to provide a submission to the Consultation process into the best way to uplift the cyber security of Australian businesses.

As an interested stakeholder, we provide feedback in the following pages on some (but not all) of the questions posed by Home Affairs in the consultation paper.

We would welcome any questions or clarification requests about our feedback.

Yours faithfully

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

Nicholas Nuske
Director and Co-CEO

About VeroGuard Systems

VeroGuard Systems Pty Limited is a cyber security company with a head office in Melbourne, Australia and a significant manufacturing facility in Edinburgh, South Australia. The VeroGuard platform was initially developed and patented by Daniel Elbaum in 2003. The platform successfully brought the security protocols for interbank communications to the internet (anywhere globally) for the first time and, by 2011, was certified in trials with banks **across** three Asia Pacific countries. In 2016, recognising the significant opportunity to solve the world's most pressing issue for online security (identity credential compromise), Elbaum successfully adapted the platform as a full identity layer for the internet to provide the first and only non-repudiable Digital Identity for guaranteed ID online.

VeroGuard Systems

Strengthening Australia's cyber security regulations and incentives

Responses to A Call for Views

Chapter 2: Why should government take action?		
1.	What are the factors preventing the adoption of cyber security best practice in Australia?	Awareness is no longer an inhibitor regarding the size and significant impacts from cybercrime. We believe that the factors now preventing best practice cybersecurity are the following: • many enterprises and most small and medium size organisations are not clear about their priorities for improving their cyber security posture (ie in what order should they adopt the essential eight?); • government should be the exemplar of what is best practice and also adopt significantly greater local content to build national capability and demonstrate best practice (ie accelerate local certifications through ACSC and trial new local solutions across agencies similar to programs in the USA and UK); and • government should be building robust shared cyber security infrastructure that will provide stronger supply chains and citizen protection, so allowing organisations and citizens the ability to utilise core cybersecurity (ie a robust digital identity).
2.	Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?	Yes. We believe that the Australian Government can (and for the first time has the opportunity to) assert leadership in establishing infrastructure which **prevents** (as opposed to detects and reports on) identity theft and data breaches for all Australians. The focus of existing frameworks and solutions are substantively around detection and remediation rather than absolute prevention. Only infrastructure that actively prevents identity and data theft will provide a broad protection for all Australians. The Government should provide a robust platform for digital identity with absolute protection of identities and sensitive data as the core component of trust to communicating and transacting online. The platform should feature: • non-repudiable digital identity and data security which does not allow decryption by unauthorised users and which does not compromise agreed privacy standards; and • cyber security upgrades which prevent incursion to critical infrastructure assets (including Security Agencies). As witnessed in the high-profile global breaches in 2021, software layers of security are proving to be ineffective, including two factor authentication, and detection software is frequently being circumvented with the average time to detection for organisations now at 209 days. Rather than persisting with more software layers that will continue to be breached by cyber criminals, the government and industry must recognise the opportunity to work with and support independent (out of band) hardware with PIN solutions for security. This has been the approach and recommendation by NIST in the US since 2019. Best practice of this technology already exists and is sovereign to Australia. The example is the VeroGuard Platform developed and being rolled out by VeroGuard Systems. In short: • the VeroGuard Platform utilises hardware security modules (HSMs); • at one end of the system, it has a personal HSM card device (the VeroCard) that has the end user's ID attached to the card and, at the other end, there is a central HSM (the VeroGuard Network) that the VeroCard communicates with over open networks; and • each time a VeroCard communicates, it generates a one-time triple encrypted message to verify and authenticate the end users' identity BEFORE the end user's own device (computer, smartphone etc) is permitted to enter the protected environment it is seeking access to (a network, a device etc).

		Systems such as the VeroGuard Platform have previously only ever been available for the highest level of secure transmissions on closed communications, such as in inter-banking transactions and for guided missile systems. The VeroGuard Platform ensures that only authorised and known (ie authenticated) persons get access. That stops any external threat attempt and ensures that only authorised persons are ever able to access systems or data. In addition, the VeroGuard Platform ensures that data at rest in the Cloud is protected. It does so as follows: • the VeroVault service (a Cloud based data security system developed by VeroGuard Systems in conjunction with CSIRO/Data 61) is an application that can then be accessed using a VeroCard; and • VeroVault enables all of the data of an end user that is sitting at rest anywhere in the Cloud to be secured and encrypted so that it is only accessible using the VeroCard as used by the end user. That effectively and completely protects the personal information of that end user. End users would each have one VeroCard which would be used by that person to securely access each service, network etc they have permission to access and to secure their data in the Cloud. By adopting the VeroGuard Platform as the standard for identity and data security, the Australian Government can immediately: • provide a zero trust security environment to each user for each transaction they undertake; • establish secure identity and standards for data at rest that cannot be decrypted by unauthorised users; • ensure that cyber policy is regularly updated to reflect the rapidly changing threats of the many levels of cyber risks and crimes; • put the control of a user's digital identity and their privacy into their own hands; • develop and implement new protocols for open network security; and • ensure that critical infrastructure assets have immediate upgrades to enable absolute full cyber threat prevention (ie Machine ID, communication and data).
Chapter 3: The current regulatory framework		
3.	What are the strengths and limitations of Australia's current regulatory framework for cyber security?	The existing regulatory framework for cyber security does not adequately enable effective governance of cyber security risks. The problem with a cyber security code being housed under the Privacy Act is that the Privacy Act deals with personal information, whereas successful cyber standards should be directed at the hardware environments that enable data to be protected so that personal information is not compromised. The Privacy Act and such cyber requirements do not sit comfortably together. The same can be said for the ACL and the Corporations Act.
4.	How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?	The best approach for strengthening corporate governance and the regulatory environment for cyber security risk is the establishment of standalone legalisation that is dedicated to cyber security and draws together the threads that are not already dealt with in the Privacy Act, the Australian Consumer Law and the Corporations Act (**Cyber Act**). The Cyber Act would establish cyber security protocols and levels (ie lowest to highest) (**Standards**). Vendors of cyber products would be required to determine the level that their product conforms to and then label their product to show consumers what that level is. The Standards would become reference points for consumers to transparently determine the performance and effectiveness of readily available cyber security products and, so, empower a consumer to confidently choose an appropriate product at the preferred security level based on the Standards.

		Presumably, the Standards would have varying gradings based on activity types. If a business held personal information of third parties, for instance, there would be a minimum Standard of cyber security product that would be required to be used by the business to protect that information to ensure the business was in compliance with the Standard. If the business does so, it would use that adoption as evidence of compliance with APP 11, the ACL and its obligations under the Corporations Act. If the business does not use cyber security products that meet the minimum Standard, then the business may be in breach of its obligations under APP 11, the ACL and the Corporations Act. The Cyber Act would enable the government to address existing and future cyber risks and developments in the one place, leading to consumer clarity of where the obligations sit and blanket coverage of all requirements. If the obligations are spread throughout none-specific legislation, there is a significant risk that consumers will be confused and to what applies and will often inadvertently miss an obligation. Enforcement would then be more easily achievable as all obligations would sit in the one place and penalties could be tailored to breaches of those obligations.
Chapter 4: Governance standards for large businesses		
5.	What is the best approach to strengthening corporate governance of cyber security risk? Why?	Option 1 – Voluntary Governance Standards The voluntary Standard would not be one adopted by a business, but would be the Standards set out in the Cyber Act (see above). The voluntary aspect would be that the Standards in the Cyber Act will not be mandatory. Provided that the co-design process is sufficiently robust, the Cyber Act Standards would provide the guidance that boards would need to consider when making cyber security product acquisition decisions. The Standards would inform board decisions and, if a board takes a voluntary decision not to implement a minimum Standard, the board would be on notice of the risk of doing so and the Cyber Act and other legislation such as the Privacy Act etc would provide enforcement mechanisms for that decision if there was loss associated with the decision. But, the decision would, ultimately, still be a commercial decision for the board weighing up all factors. We agree that care will need to be taken to ensure that a voluntary Standard does not promote a 'tick-a-box compliance culture', where businesses do not critically assess their security requirements.
6.	What cyber security support, if any, should be provided to directors of small and medium companies?	Directors should be provided guidance and tools to allow them to determine priorities for their business regarding need-to-know standards, risk profiles and capability levels for cyber security. Small and medium business and, therefore, their Directors should also be able to access core digital identity infrastructure in support of securing their supply chains.
7.	Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?	Cyber-crime is now a significant issue for business continuity. Business leaders need greater guidance on the steps and priorities for securing their systems and data when they are exposed online. The education should include what are the core risks they face, capabilities they should have and standards they need to adopt.
Chapter 5: Minimum standards for personal information		
8.	Would a cyber security code under the Privacy Act be an	No, see comments above. The cyber security code needs to be a separate Cyber Act.

	effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?	
9.	What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?	Yes. Organisations would need to understand what technical controls need to be in place to comply.
10.	What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?	The Cyber Act must make the use of multi-factor authentication mandatory. And this should be set at a standard of hardware-based security utilising certified HSM to HSM authentication and communication. This should require the use of a platform to enable them to authenticate their identity to protect networks and data. By doing this, cyber security resilience can be raised across the economy by accelerating the adoption of technical standards. See the answer in Chapter 2.
Chapter 6: Standards for smart devices		
11.	What is the best approach to strengthening the cyber security of smart devices in Australia? Why?	As for personal identity protection, we believe that the Australian Government can (and for the first time has the opportunity to) assert leadership in establishing infrastructure which **prevents** (as opposed to detects and reports on) unauthorised access to and data breaches for smart devices by only adopting hardware-based authentication via HSM to HSM communication. HSM to HSM communication will be critical to secure and simplify Australia's online communications. An example of world leading sovereign capability that already exists is, again, the VeroGuard Platform developed and being rolled out by VeroGuard Systems (see answer to (2) above). As for the protection of human transactions, the VeroGuard Platform can protect machine transactions on the IoT as follows: • at one end of the system, there is a machine HSM device (the VeroMod); • a smart device's ID is attached to the VeroMod; • the authentication of the user accessing apps via the smart device can also be done with a personal HSM (a VeroCard) and the central HSM (the VeroGuard Network); • the VeroMod/VeroCard communicates with over open networks using, each time, a one-time triple encrypted message to verify and authenticate the smart device's identity BEFORE the party authorised by the VeroMod/VeroCard is permitted to access the protected environment; • the VeroVault service then enables all of the data generated by the machine protected by a VeroMod (for instance, security footage from a security camera) to be sent to and sit at rest anywhere in the Cloud and then be secured and encrypted so that it is only accessible using a VeroCard as used by an authorised end user. That

		effectively and completely protects the camera, the data authenticity and the data in transit generated by that machine; • one VeroMod would be connected in line with each machine isolating the machine from the open network; and • the operators of the network of machines protected by the VeroMods would have VeroCards which would be used to securely access and control for each VeroMod they have permission to access. By adopting the VeroGuard Platform and VeroMods as the standard for identity and data security, the Australian Government could immediately: • provide a zero trust security environment to each smart device supported; • establish secure identity and standards for data at rest that cannot be decrypted by unauthorised users; • ensure that cyber policy is regularly updated to reflect the rapidly changing threats of the many levels of cyber risks and crimes; • develop and implement new protocols for open network security; and • ensure that critical infrastructure assets have immediate upgrades to enable absolute full cyber threat prevention (ie Machine ID, communication and data).
12.	Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt for as a standard for smart devices? a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate? b. If not, what standard should be considered?	We believe that the standard is a good start. If ESTI EN 303 645 is to be adopted, it should be adopted in full and not lag the global standards in Australia.
13.		No response
14.		No response
15.		No response
Chapter 7: Labelling for smart devices		
16.		No response
17.		No response

18.		No response
19.		No response
20.		No response
21.		No response
Chapter 8: Responsible disclosure policies		
22.	Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?	No response
Chapter 9: Health checks for small businesses		
23.	Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?	Providing small and medium business a health check is a marginal activity if not supported by robust digital identity infrastructure to eliminate credential compromise and create an environment where any other cyber security measures may be deployed. It is critical to reinforce the need for hardware-based multi-factor authentication and a tethered secure ID for each person and business to guarantee provenance of every access request and communication for business and government interacting online. The Australian Business Number (ABN) already has a single business identifier with the ABN register. There is a substantial opportunity to leverage existing investments by the ATO to deliver rapidly secure guaranteed business ID for the chance to: • provide business with the ability to securely access multiple government tender sites and applications with their unique unified and absolutely secure Digital ID; • give confidence and trust for business and government when working together online; • eliminate business email compromises; • protect businesses from espionage, theft and malicious ransom attacks utilising split encrypted multi-server ultra-secure storage for government data and corporate profiles, information and proposals; • improve efficiency for business and government by: o eliminating duplication; o delivering absolute trust when supplying, storing and working with sensitive tender information for government and suppliers; o delivering a single identity for business across multiple tender sites, rationalising for business and government; o securely and privately pre-populating common information;

		o bring all business and government to Protected levels of cyber security for sensitive data; o removing many risks, such as GPDR breaches; and o having a common and re-usable platform, developed to comply at the highest levels with DTA framework.
24.	Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?	As per above (23)
25.	If there anything else we should consider in the design of a health check program?	As per above (23)
Chapter 10: Clear legal remedies for consumers		
26.		No response
27.		No response
Chapter 11: Other issues		
28.	What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?	Two key points we would add are: 1. whilst cyber security is a shared responsibility, there are significant opportunities for Government to lead with clear policies and regulations that will benefit and protect Australian business, citizens and critical infrastructure. The policies and regulations will always fall short, however, if not underpinned with Government leading with robust infrastructure connecting business and citizens to government and with each other (for example, a trusted identity layer for the internet); and 2. rights of consumers will count for little if cyber criminals, particularly from outside our physical borders, can instigate economic or information loss by assuming the identity of the consumers and or their connected machines. Policies and rights can only be as effective as the core technology protections provided in cyber environments.