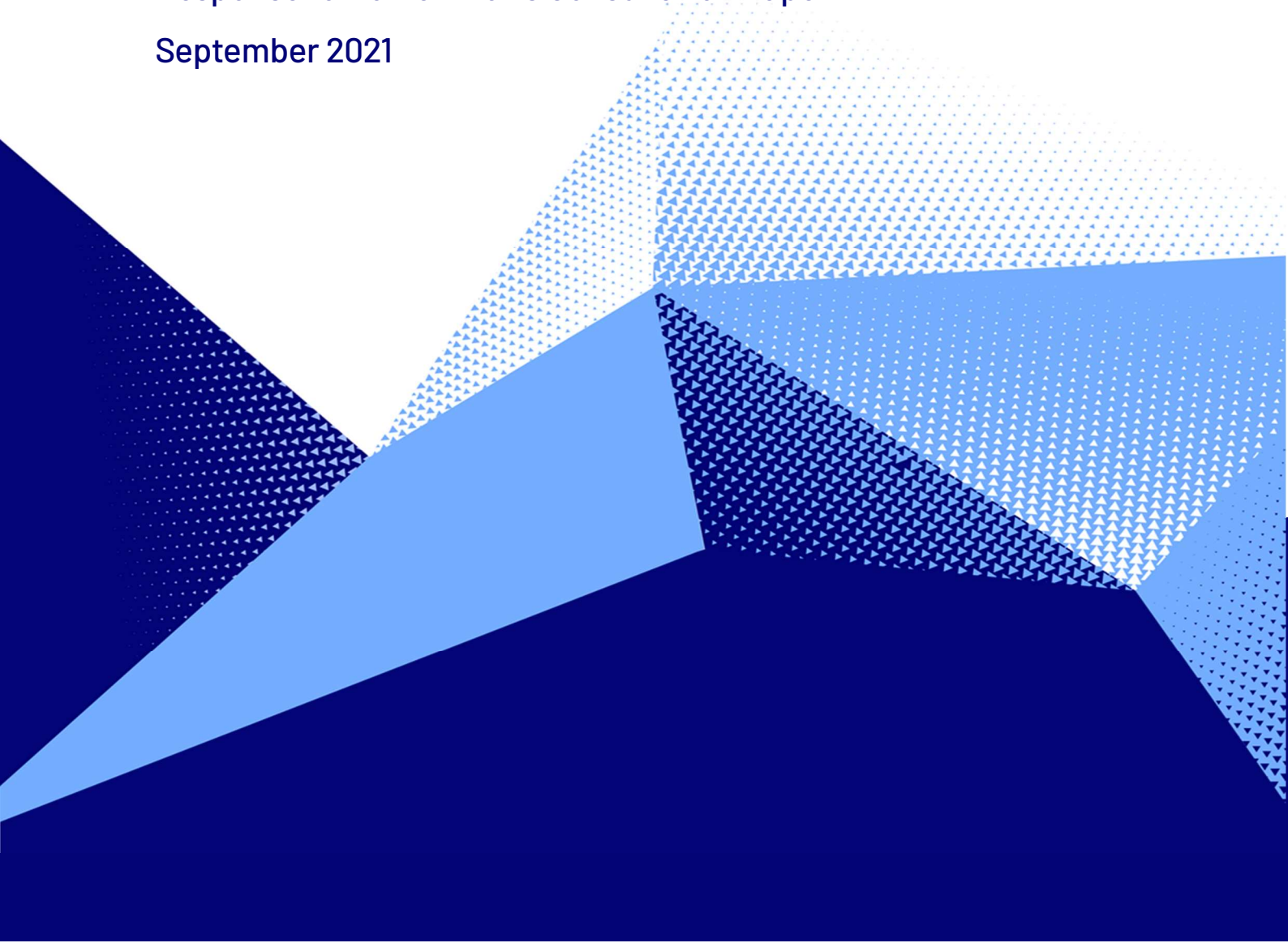
CyberCX

Strengthening Australia's cyber security regulations and incentives

Response to Home Affairs Consultation Paper

September 2021



1 Overview

CyberCX, as Australia's largest cyber security professional services company, welcomes the opportunity to respond to the Australian Government's call for views on *Strengthening Australia's Cyber Security Regulations and Incentives* (**Paper**).

Our submission is based on CyberCX's significant operational and advisory experience including:

- Direct experience from cyber incidents managed by our Digital Forensics & Incident Response (DFIR) practice.
- Operational insights from CyberCX's Security Testing & Assurance (STA) practice, the largest security testing capability in the region, and telemetry collected by our Managed Security Services (MSS) teams across 100+ major Australian networks.
- Expert interviews with our Strategy & Consulting (S&C) and Governance, Risk & Compliance (GRC) experts on how Australia's leading organisations protect their most critical assets and manage cyber risk.
- Our uniquely Australia and New Zealand focused Cyber Intelligence team, which leverages high quality closed and open source feeds, plus dark web monitoring.

2 General feedback

CyberCX strongly supports the Paper's intent to achieve whole-of-economy cyber security uplift via outcomes-based market mechanisms. We have five overarching areas of feedback, outlined below. In Part 3 we provide further detail on how each overarching concern maps against specific policy proposals tested in the Paper.

1. **Drive cost into the right market:** Lifting Australia's cyber security needs to be achieved via a genuine compact between government and industry. Most policy proposals outlined in the Paper will involve cost to business and, in many cases, consumers. It's important that cyber risk is appropriately priced into the market, but increased expectations on Australian organisations must be accompanied by more law enforcement action to make Australia a less permissive environment for cybercriminals. ***CyberCX urges the Australian Government to further prioritise and scale up law enforcement efforts to drive cost into the business models of cybercriminals.***

2. **Investment in regulatory capability:** A number of the Paper's proposals anticipate a stronger role for regulatory, certification or enforcement bodies. Other proposals would be strengthened by clearer mechanisms for government to co-design and dynamically update standards, assist organisations to understand and meet their obligations and, where necessary, identify non-compliance and enforce standards. A new regulatory body with appropriate resources and powers may be required to ensure a number of the Paper's proposals are effective, similar to the role ASIC plays for the financial system. Alternatively, an existing regulatory body could fill this role, provided it was given capability and capacity to do so. In the absence of new regulatory models, the Department may need to contemplate how private sector organisations could be used to fulfil certification, testing and other roles. ***CyberCX urges the Department to consider and to continue to consult on the best regulatory model for the Paper's policy proposals.***

3. **Education and awareness campaigns:** Many of the proposals contemplated will not drive consumer behaviour change in the desired way unless accompanied by targeted, effective information and awareness campaigns. Indeed, without focused consumer education some of the proposals may perversely drive price-sensitive consumers away from safer products. ***CyberCX urges the Department to continue to consult with industry and consumer groups on the most effective and efficient consumer awareness approaches.***

4. **Driving real behaviour change, not a compliance approach:** CyberCX strongly agrees that there is a need for a significant uplift in cyber security across the economy. Indeed, Australia's cyber threat landscape is worsening, with disruptive, costly cybercrime such as ransomware impacting more organisations across all sectors. An incremental approach to this problem is destined to fail; the highly adaptive nature of threat actors and rapidly changing technology environment require a broadscale, coordinated effort across government and industry. Further, if not properly calibrated, there is a risk that enhanced standards could simply entrench current practices, encourage a 'checkbox' approach to compliance, or stimulate risk shifting in the economy (e.g. through the writing of directors' liability insurance). ***CyberCX urges the Department to continue working with industry and consumer groups to ensure that proposals will trigger significant, desirable behaviour change.***

5. **Regulatory duplication and competing standards:** Aligned to ongoing consultation on the implementation of the Security of Critical Infrastructure reforms, there is a need for Home Affairs to continue to drive harmonisation and simplification across various federal and state legislative and regulatory regimes.

3 Specific feedback

Proposal	Feedback
Enhanced board governance standards	CyberCX supports strengthening corporate governance of cyber security risk. We urge the Department to continue to work with industry to develop new governance standards that will result in a genuine step-change in cyber resilience across the economy. For example, there is a risk that frameworks based on meeting 'market standards' will entrench the status quo, rather than drive change. Or that new standards will result in a checkbox compliance mentality, rather than a proactive approach to managing risk. The role of directors' liability and cyber insurance needs to also be carefully considered, as it can de-motivate appropriate investment. Further, new standards will not achieve their full potential unless coupled with clear, well-resourced mechanisms for ensuring accountability. Currently, regulators lack the cyber capability and personnel needed to assess compliance. A regulator-led approach should not just be enforcement based—regulators involved would need a mandate to proactively help organisations meet their obligations, for example by issuing guidance and rulings. Finally, the Department should carefully consider who is able to take action when standards are not met, and through what legal means. Consumers have limited power to take action against large corporations; smaller shareholders may be similarly disempowered. Additionally, it is important to ensure that any cyber-specific governance standards do not duplicate or conflict with obligations that may already exist for businesses operating within industries with existing regulatory requirements. Finally, CyberCX strongly believes that there needs to be a compact between industry and government on cyber security. It's imperative that enhancing governance standards (which will increase cost to business) occurs alongside a reciprocal uplift in services from law enforcement and others across government.
Minimum standards for personal information	Good privacy practices are intrinsically linked to improving broader cyber security outcomes. CyberCX supports government more closely considering how the role of the Office of the Australian Information Commissioner (OAIC) can complement cyber security efforts across the economy including via empowering the OAIC to upgrade its guidance on securing personal information to an enforceable Code, mandating best practice for businesses in securing the personal information they collect and hold. However, empowering the regulator with 'sharper teeth' would arguably do more to uplift compliance with best practice information security standards than any Code under the current *Privacy Act*. This could include reforms to the *Privacy Act 1988* to empower the OAIC to impose greater sanctions for the most egregious offenders. The way in which the prudential sector is held to a high standard of

Proposal	Feedback
	compliance with its obligations under Prudential Standard CPS 234 is instructive as to how an appropriately empowered regulator can be drive uplift and compliance with privacy best practice.
Mandatory minimum standards for smart devices applied to manufacturers & sellers	For standards to drive significant behaviour change, there is likely to be a need for greater regulatory capacity within government – or appropriately certified third parties – to ensure that labelled products are appropriately assessed against the agreed standards and that compliance is audited and enforced. There is also a need for consumer rights and remedies for IoT and digital products to be more clearly defined. At a minimum, standards should cover: automated security updates, length of time a device is supported with updates, encryption on network traffic, authentication methods and storage standards. We agree that the cost to industry of testing and certifying products will be relatively modest – since IoT devices are sold at scale. To mitigate unintended consequences, working with other like-minded countries on standard-setting will be key. If Australia sets standards above those of other countries then this could mean we are unable to get products available to other regions and we could be left behind in new technologies. (We are already behind on Wi-Fi 6E due to spectrum issues.) Aligning ourselves with like-minded countries will increase the buying power of countries wanting better standards and therefore the likelihood of products being available in Australia.
Labelling for smart devices	We support a combination of standards and labelling for smart devices and suggest a phased approach which begins with voluntary standards. However, a number of significant shifts are needed before this regime could be mandatory – and to ensure voluntary standards will achieve the desired behavioural change: ▷ **Consumer awareness.** Unlike energy efficiency ratings that translate into direct energy savings for consumers, the benefits of safe smart devices are much more diffuse (and some – for example, hardening a device so it is not recruited into a criminal botnet – are often not enjoyed by the end-user themselves). Education and awareness will be crucial to ensuring that consumers appropriately factor safety into their purchasing decisions and understand the meaning of labels. ▷ **Consumer empowerment.** The Department should consider ensuring that labels provide simple instructions to consumers about *how* to operationalise any security features contained on the device and provide clear advice on remedial action open to them. Certain mandatory notifications after purchase could also be helpful (via pop-ups on devices, an enrolled consumer email, or on the supplier's website). For example, consumers should receive a reminder when updating and support will soon cease. ▷ **Regulatory capacity and oversight.** Labelling reinforces the need (discussed above) for sufficient regulatory capacity to monitor and enforce standard compliance. It will be especially required if dual physical/digital labelling is adopted to facilitate regular audits and updates to labels.

Proposal	Feedback
	Further, we agree that this regime should extend to mobile phones – given these hold the majority of all consumers' most sensitive personal information and communications, and consumers are increasingly being victimised via mobile phone scams which take advantage of poor device security configurations. Digital labelling should be sufficient as physical labelling of some devices will be practically difficult. Regardless, labels should be dynamic. (For example, devices could have a physical sticker and link to a website, where after products are periodically reviewed against standards, labels are adjusted.) Finally, we note that appropriate labelling for consumer devices may not be appropriate for small-to-medium enterprises. While it is appropriate to assume that consumers will not do device maintenance, and so updates should occur via default, a 'good' device from an enterprise perspective will offer more control over updates and patching timing, and provide some capability for control over device maintenance.
Voluntary vulnerability disclosure policies for software developers and businesses providing services online	Voluntary standards will have some positive benefit and should be principles-based to enable organisations tailor their policy to reflect their operational environment. However, CyberCX believes that there are more effective ways to achieve desired behaviour change in the vulnerability marketplace. Namely: ▷ CyberCX urges the Australian Government to lead by example on voluntary disclosure. A clear, Whole-of-Government Voluntary Disclosure Policy that creates a single portal for researchers to share vulnerabilities found in government systems, clarifies when and how researchers will be rewarded or recognised, and clarifies issues around researcher liability, would set a powerful example in market, while also helping to better secure federal government systems. ▷ The Department should consider ways to change market incentives for security researchers and others who find vulnerabilities. The market for exploits continues to be profitable for researchers. To alter incentives, the Department could consider professional standards or ethical guidance for security researchers. It should also consider how legal frameworks apply to those who sell vulnerabilities to third parties, or release proof of concept code before a vulnerability is patched. For example, the 2021 release of technical details for the ProxyLogon vulnerability in the Microsoft Exchange Server by a security researcher directly contributed to active scanning and exploitation of this vulnerability by multiple threat actors, leading to the victimisation of Australian organisations. Finally, the Department may wish to look at ways to link any vulnerability disclosure regime with the proposed new standards and labelling of IoT devices. For example, if the Department chooses to authorise one or more regulators or organisations to certify IoT devices, these same bodies could become places to report unpatched vulnerabilities. If the vendor does not take reasonable steps to patch or develop a work-around within appropriate timeframes, product safety labels would be affected.

Proposal	Feedback
Voluntary health checks for small businesses	Lifting the cyber security capability and awareness of small business will have positive impacts on supply chain risk and be hugely beneficial for Australian consumers. However, the endemic set of challenges for small business which the Department acknowledges – limited time, money, and cyber security baseline expertise – pose a risk to the success of a light-touch approach to this problem. The dilemma is that it is unsustainable for small businesses to comply with a set of mandatory cyber security requirements, yet a voluntary model based on self-assessment may result in a checkbox compliance culture and sense of complacency from businesses and consumers who place their trust in a health check trust mark. The detail around administration and maintenance of a voluntary scheme will largely determine its success. ▷ A successful voluntary scheme will need to be easy to engage with, provide a strong value exchange proposition for participants and offer supported pathways toward higher degrees of cyber maturity. ▷ There are lessons to be gleaned in this regard from the UK Cyber Essentials model, including which bodies are empowered to certify businesses and the tiered model for more mature organisations (Cyber Essentials Plus). ▷ Consideration should also be given to coordinating with other government initiatives on cyber awareness and education. For example, CyberCX, with funding from the Department of Industry, Science, Energy and Resources, is developing a program, Cyber123 for SMEs, that helps improve the cybersecurity awareness and skills of small-to medium enterprises. The feedback we consistently hear from SMEs is that there is a need and an appetite for easily accessible, modular, on-demand learning and upskilling resources for SMEs to improve their cyber security posture.

4 Other issues

CyberCX is of the view that the following must be considered in any effort to strengthen Australia's cyber security regulation and incentives.

- **Cleaner Pipes**

  The *Cyber Security Strategy 2020* outlined a commitment to support businesses to implement threat-blocking technology that can automatically protect businesses and citizens from malicious online content and malware. Telstra has announced and implemented its own Cleaner Pipes initiative which leverages Domain Name System filtering to automatically block millions of malware communications detected on Telstra's infrastructure every week.

  CyberCX strongly supports the Cleaner Pipes model and encourages government to consider how it might play a more proactive role in incentivising relevant businesses –

primarily telecommunications and internet service providers – to adopt DNS filtering. We also urge government to explore options for internet, email, SMS and call filtering.

Cyber security is a volume crime: cybercriminals scale their attacks to target millions of potential victims. Broad adoption of threat-blocking technology will vastly reduce the volume of these attacks, providing benefits for consumers, lifting the baseline of security for every internet user in Australia, and allow law enforcement to focus on the most serious and persistent threats.

- **Cyber insurance**

  Cyber insurance policies have significant potential to incentivise cyber security uplift; but a distorted market can also dampen signals to businesses. CyberCX suggests that the Department should consider the role that the cyber insurance market plays in exacerbating or ameliorating negative externalities and information asymmetries, and how the industry might affect the effectiveness of proposals raised in the Paper.

CyberCX would welcome working with the Department of Home Affairs as the policy proposals outlined in the Paper are further developed. For further information on this submission, please contact us directly:

Jordan Newnham
Director—Communications and Government Relations
[redacted]

Katherine Mansted
Director—Cyber Intelligence and Public Policy
[redacted]

About CyberCX

CyberCX is Australia and New Zealand's leading provider of professional cyber security services. With a workforce of over 900 professionals, we help private and public sector organisations realise the opportunity of improved cyber security in an increasingly complex and challenging threat environment. CyberCX offers a comprehensive set of services across nine practices:

- Identity & Access Management
- Managed Security Services
- Digital Forensics & Incident Response
- Cyber Capability, Education & Training
- Strategy & Consulting
- Security Testing & Assurance
- Governance, Risk & Compliance
- Security Integration & Engineering
- Secure Digital Transformation