AustCyber
Australian Cyber Security Growth Network

SUBMISSION

STRENGTHENING AUSTRALIA’S CYBER SECURITY REGULATIONS AND INCENTIVES

DISCUSSION PAPER
DEPARTMENT OF HOME AFFAIRS
AUGUST 2021

Cyber security: a critical enabler for all Australians

We agree that much can be done to further strengthen Australia's collective cyber security posture and that of individual organisations. We acknowledge the growing threat surface, and specific sources of vulnerability, as outlined by the Australian Government and our allies and security partners, over recent years.[1,2]

Prior to the COVID-19 pandemic unfolding, cyber security was at a critical inflection point in the Australian economy as both a foundational element of doing business and in its maturity as an industry providing economic benefit as well as delivering the capabilities needed to defend against malicious cyber activity. The pandemic has of course only compounded this, but also afforded the nation an opportunity to better understand the role and practice of cyber security – and its relationship with privacy.

In this submission, we limit our comments to the specific proposals outlined in the Discussion Paper presented by the Department of Home Affairs, *Strengthening Australia's Cyber Security Regulations and Incentives*.

In making this submission, we draw attention to the intersecting proposals for amendments to the Security of Critical Infrastructure Act 2018 *Cth*, currently before the Parliamentary Joint Committee on Intelligence and Security (PJCIS), which has potential implications for supply chains and broad segments of the Australian economy. We are of the view that any measures adopted, as envisaged by the Discussion Paper, should ensure **harmonisation**. This includes a focus on recognised international standards, with a view to ensuring market entry is facilitated for Australian companies seeking to export to trusted markets.

We look forward to working with the Department on this issue of importance to the country, as it considers submissions and specific policy proposals.

1. Governance for large businesses

The need for coherent, fit-for-purpose, cyber security standards has always been clear internationally. These arguably already exist, through recognised international standards, including those developed jointly by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), and adopted in Australia.

ISO/IEC 27001, for example, provides a broad management system for information security.[3] Similarly, more generic risk management standards, such as ISO 31000, initially developed with significant contributions from both Australia and New Zealand, provide an internationally relevant approach to risk management, for entities of all sizes. At the time of publication, ISO 31000 is available for viewing, free to the user, on the ISO website.[4]

In addition, the Australia Prudential Regulation Authority (APRA) and other regulatory bodies have developed standards for specific sectors of the economy, with implications for Boards, including from an oversight perspective.[5] One example is APRA CPS 234. As such, the need to develop new

[1] Office of the Director of National Intelligence. (2021). 'Annual Threat Assessment: Opening Statement,' accessed 30/08/2021 from: https://www.dni.gov/files/documents/Newsroom/Testimonies/2021-04-14-ATA-Opening-Statement-FINAL.pdf
[2] ASIO (2020). *Annual Report 2019-20.* Canberra: Commonwealth of Australia.
[3] Standards Australia (2021). *Recommendations Report: NSW Cyber Security Standards Harmonisation Taskforce. Sydney: Standards Australia.*
[4] https://www.iso.org/standard/65694.html
[5] APRA (2021). 'Information Security', accessed 30/08/2021 from: https://www.apra.gov.au/information-security

governance standards is not well evidenced, given that many existing standards address this area of focus, in addition to other areas.

Uptake of these standards has varied in Australia, with regulated sectors such as financial services and telecommunications, traditionally being early adopters of standards at-scale, including within commercial supply chains. Clearly, this practice is not the experience of a wide range of other sectors. Part of the explanation for this reality might be additive costs related to certification, and a lack of awareness and/or understanding of the complexities in the practice of cyber security.

Government policy intervention can clearly, and decisively, address the second part of this dilemma – by making information more readily available, easy to understand and tailored to the requirements of businesses of different sizes with different ambitions, i.e. exporters versus those who do not have an export focus. As we noted in the 2021 report of the NSW Cyber Security Standards Harmonisation Taskforce:

> *Care must be taken to factor-in how standards are to be used, for what purposes and in relation to specific public policy requirements. This might include consideration of the relative merits of principles- based approaches, attestation, certification and how development, adoption or use of standards might impact supply chains or procurement behaviour.*[6]

In our view, a constructive contribution from Government would be to raise awareness and promote the use of recognised international standards, as the Discussion Paper acknowledges.[7]

This might include, for example, the development of an industry co-developed guide that maps the standards that exist in different domains (i.e. protective security, information security etc.) and addresses current information asymmetries in this area. Such a guide could assist entities of all sizes to identify, select and use standards that are relevant to them, preserving the integrity of supply chains and raising baseline cyber security posture. This would meet the objectives of *Australia's Cyber Security Strategy 2020* and recognise the existing good practice that exists across the digital economy, including where responsible companies are proactively taking measures to enhance cyber security.

Recommendation: Building on the work across industries undertaken by the NSW Cyber Security Standards Harmonisation Taskforce, the Australian Government should address the information asymmetries that exist concerning cyber security standards nationally by developing a coherent guide that identifies, maps and explains the various cyber security standards in existence, and their applicability to businesses and entities of all sizes. Such a guide would benefit from also providing case studies to support its wide use.

2. Minimum standards for protection of personal information

We acknowledge that personal information protection should be a priority for the Australian Government, as well as for the private sector. The introduction of the Notifiable Data Breaches Scheme has assisted in raising both awareness of the criticality of personal information, as well as encouraging reporting and accountability for breaches.[8] Many large companies also have extensive policies and frameworks concerning both information security and privacy management, central to personal information protection.

[6] Standards Australia (2021). *Recommendations Report: NSW Cyber Security Standards Harmonisation Taskforce. Sydney: Standards Australia*, p. 7.

[7] Department of Home Affairs (2021). *Strengthening Australia's cyber security regulations and incentives.* Canberra: Commonwealth of Australia, p .64.

[8] OAIC (2021). 'About the Notifiable Data Breaches scheme', accessed 31/08/2021 from: https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/. We note that in our discussions with a range of non profits and associations in non technology orientated industries that awareness of the Notifiable Data Breaches Scheme remains low overall.

As the Discussion Paper notes, the Privacy Act 1988 *Cth* is subject to a review, which may have broad implications for the digital economy. This review assumes added significance in relation to cross-border data flows, and digital services exports, as countries explore adequacy mechanisms and other arrangements.

While not opposed to an industry-led code under the Privacy Act 1988 *Cth*, we would need clarity on the contents of any such code and a clear understanding of the extent to which it intersects with mandatory obligations, were the passage of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* to be secured, as well as any voluntary measures already in existence. Were the Department to proceed with a code that includes technical standards, we suggest that consultation with industry take place to determine the most widely used standards, and therefore those that are more likely to be effective, prior to them being referenced in any such code.

Recommendation: We do not have an objection to a well-researched, industry-led process for a code, but note the need to consider the plethora of existing tools that seek to achieve similar objectives.

3. Standards for security of smart devices

Standards for smart devices, and more specifically Internet of Thing (IoT) devices, have long been acknowledged as necessary and overdue.

We note the considerable efforts that have been made by conscientious local companies, and responsible global companies, to ensure the safety and security of IoT devices, including through standards-based approaches, in recent years.[9]

In terms of promoting the adoption of a new standard, we are supportive of the adoption of industry-led standards. ETSI EN 303 645 is one such example.

Were the Government to adopt any standards through regulatory call-up, we would recommend a Regulatory Impact Statement (RIS) be developed. Furthermore, the Government might wish to consider the architecture of other statutory mechanisms, including the Water Efficiency Labelling Scheme (WELS), to guide its considerations.[10]

Were Government to proceed, and broadly consistent with this approach, it would be preferable for Government to manage the architecture of the scheme, whilst operational aspects can be delegated to a National Standards Body, such as Standards Australia. Accordingly, adoption of the standard and the development of technical measures required in-market to accompany its implementation, can be managed by the National Standards Body.

4. Responsible disclosure policies

Increasingly, entities are recognising the importance of well-considered vulnerability disclosure policies and AustCyber has long been an advocate for the wide adoption of such policies. This includes advocating for the approaches taken by Bugcrowd and others on building and sustaining curated ecosystems and transparent methodologies to achieve desired outcomes, which have been proven to also deliver second and third order benefits.

In the past, three key barriers to reporting vulnerabilities have been identified. These include: (1) uncertainty in how to report a vulnerability, (2) lack of confidence in the vulnerability being fixed and (3) uncertainty or fear around consequent legal action.[11]

[9] Shankland, S. (2021). 'Google, Amazon, Apple back Matter standard so smart home devices cooperate,' accessed 31/08/2021 from: https://www.cnet.com/home/smart-home/google-amazon-apple-back-matter-standard-so-smart-home-devices-cooperate/

[10] WELS Regulator (2021). 'Water Rating,' accessed 31/08/2021 from: https://www.waterrating.gov.au

[11] United States Department of Homeland Security (2020). 'Binding Operational Directive 20-01', accessed 31/08/2021 from: https://cyber.dhs.gov/bod/20-01/

In the 2021 Recommendations Report of the NSW Cyber Security Standards Harmonisation Taskforce, we recommended that stakeholders, including Government, consider leveraging the following documents in developing comprehensive vulnerability disclosure policies, frameworks and resources:

- US Homeland Security Binding Operational Directive 20-01
- IEC 29147:2018, *Information technology — Security techniques — Vulnerability disclosure*

We support the intent of the Discussion Paper in making resources to facilitate vulnerability disclosure more widely available to Australians.

Recommendation: AustCyber supports option 1 – concerning voluntary approaches to increasing responsible disclosure. The Department should engage with industry on how existing frameworks in this area can be leveraged and complement other cyber risk mitigation strategies.

5. Health checks for small business

Aside from audits and certification, there are a range of cyber health check models for businesses in existence, including SMEs, though uptake varies. The Department should seek to leverage these in developing any approach, including through exploring how existing good practice can be recognised through a ‘trust mark’ approach, as outlined in the Discussion Paper.

In early 2021, the Department of Industry, Science, Energy and Resources, announced the recipients of the Cyber Security Business Connect and Protect grant program, including those providing services ranging from auditing through to accreditation.[12]

The NSW Cyber Security Strategy, launched in early 2021 also identified the Cyber Check.Me initiative as having particular relevance and application. This was developed by Edith Cowan University, with partners, including AustCyber.[13]

Recommendation: We support option 1, but encourage the Government to explore the range of existing service offerings within Australia that might assist to shape the way this scheme works in practice and supports concurrent incentive-orientated mechanisms.

[12] https://business.gov.au/grants-and-programs/cyber-security-business-connect-and-protect/grants-recipients
[13] https://www.ecu.edu.au/schools/science/research-activity/ecu-security-research-institute/cybercheckme

About AustCyber

As the Australian Cyber Security Growth Network Limited, AustCyber is a publicly funded, private entity which commenced on 1 January 2017. Our mission is to grow Australia's cyber security sector, to support the development of a vibrant and globally competitive Australian cyber security sector. In doing so, our activities will enhance Australia's future economic growth in a digitally enabled global economy and improve the sovereign cyber capabilities available to protect our nation's economy and community.

Our funding comes from majority Federal Government grants – funding for operations and programs, and for the $15 million AustCyber Projects Fund which provides grants to projects that deliver national benefit. We also receive funding under contracts with the governments of the ACT, NSW, QLD, SA, TAS, WA and the Sunshine Coast Regional Council and Townsville City Council, which we match, to deliver AustCyber's national network of Cyber Security Innovation Nodes – with the NT and VIC soon to join.

We work to align and scale Australian cyber security research and innovation related activities across the private sector, research communities, academia and within Australian governments. We are responsible for maintaining a strong supply of innovative Australian cyber security solutions and capability and have established ourselves as an independent advocate for the competitive and comparative advantages of Australian technical and non-technical cyber security capabilities.

Beyond our shores, we work with partners across many countries to develop export pathways for Australian solutions and capability. This helps the rapidly growing Australian cyber security sector tap into market 'hot spots' around the world.

In February 2021, we merged with Stone & Chalk Limited to form the Stone & Chalk Group, Australia's largest network of Innovation Hubs and Nodes growing globally comeptitive Australian startups and scaleups in emerging technologies.

Contacts:

Michelle Price, CEO AustCyber
[redacted]

Dr Jed Horner, Head of Government Relations & Advocacy
[redacted]